

# Modular Hyperbolas

IGOR E. SHPARLINSKI

Department of Computing, Macquarie University  
Sydney, NSW 2109, Australia  
igor.shparlinski@mq.edu.au

January 14, 2013

## Abstract

We give a survey of a variety of recent results about the distribution and some geometric properties of points  $(x, y)$  on modular hyperbolas  $xy \equiv a \pmod{m}$ . We also outline a very diverse range of applications of such results, discuss multivariate generalisations and suggest a number of open problems of different levels of difficulty.

## 1 Introduction

### 1.1 Modular Hyperbolas

For a positive integer  $m$  and an arbitrary integer  $a$  with  $\gcd(a, m) = 1$ , we consider the set of points  $(x, y)$  on the modular hyperbola

$$\mathcal{H}_{a,m} = \{(x, y) : xy \equiv a \pmod{m}\}.$$

We give a survey of various results about the distribution and some geometric properties of points on  $\mathcal{H}_{a,m}$ . We also briefly consider some multidimensional generalisations, which often require very different techniques. Several open problems are formulated as well. Our main goal is to show that although  $\mathcal{H}_{a,m}$  is defined by one of the simplest possible polynomial congruences, it exhibits many mysterious properties and very surprising links with a wide variety of classical number theoretic questions and beyond.

In this survey, we do not present complete proofs but rather explain their underlying ideas and specific ingredients. Typically the error terms in the asymptotic formulas we give contain a factor  $m^{o(1)}$ . In most cases it can be replaced by a more explicit function. Furthermore, when  $m$  is prime it can usually (but not always) be replaced by just some low power of  $\log m$ .

There is a large number of papers in this area which rather routinely study seemingly distinct, but in fact closely related, problems about  $\mathcal{H}_{a,m}$  on a case by case basis. Here, we explain some standard principles which can be used to derive these and many other results of similar spirit about the points on  $\mathcal{H}_{a,m}$  as simple corollaries of just one general result about the uniformity of distribution of points on  $\mathcal{H}_{a,m}$  in certain domains. In Section 3.1, such a result is presented in Theorem 13 and derived in a very straightforward fashion from bounds of Kloosterman sums (see (1) below) using some standard arguments. Results of this type are quite standard and can be obtained for many other curves (at least in the case of prime modulus  $m$ , where the Bombieri bound [28] provides a readily available substitute for (1)).

However, most of the other results on modular hyperbolas rely on some rather subtle number theoretic arguments which in general do not apply to other polynomial congruences. This places modular hyperbolas in a very special position and shows that they define a mathematically much richer structure than a “typical” polynomial congruence.

## 1.2 Distribution of Points and Kloosterman Sums

Since the distribution of points on  $\mathcal{H}_{a,m}$  is our primal object of study, we introduce the following definition. Given two sets of integers  $\mathcal{X}$  and  $\mathcal{Y}$ , we write

$$\mathcal{H}_{a,m}(\mathcal{X}, \mathcal{Y}) = \{(x, y) \in \mathcal{H}_{a,m} : x \in \mathcal{X}, y \in \mathcal{Y}\}.$$

Since the case of  $a = 1$  is of special interest we also write

$$\mathcal{H}_m = \mathcal{H}_{1,m}, \quad \text{and} \quad \mathcal{H}_m(\mathcal{X}, \mathcal{Y}) = \mathcal{H}_{1,m}(\mathcal{X}, \mathcal{Y}).$$

Obtaining precise asymptotic formulas for and establishing the positivity of  $\#\mathcal{H}_{a,m}(\mathcal{X}, \mathcal{Y})$  for various “interesting” sets  $\mathcal{X}$  and  $\mathcal{Y}$  have been the central themes of many works in this direction. Certainly the problem becomes harder and far more interesting when the sets  $\mathcal{X}$  and  $\mathcal{Y}$  become “thinner”.

Let

$$\mathbf{e}_m(z) = \exp(2\pi iz/m).$$

One immediately observes that the well-known bound

$$|K_m(r, s)| \leq (m \gcd(r, s, m))^{1/2+o(1)}, \quad (1)$$

of *Kloosterman sums*

$$K_m(r, s) = \sum_{\substack{(x,y) \in \mathcal{H}_m \\ 1 \leq x,y \leq m}} \mathbf{e}_m(rx + sy), \quad (2)$$

see [115, Corollary 11.12], can be used to study the points on  $\mathcal{H}_{a,m}$ . One only needs to recall some standard tools which link exponential sums with uniformity of distribution which we present in Section 2.3.

We remark that most of the results which rely only on (1) do not appeal to anything specific about the congruence  $xy \equiv a \pmod{m}$ , and at least when  $m$  prime they can be extended to the distribution of solutions to more general congruences  $f(x, y) \equiv 0 \pmod{m}$ , with a polynomial  $f$  with integer coefficients. In the case of prime  $m$ , the Bombieri bound [28] of exponential sums along a curve replaces the bound (1). Although, as we have mentioned, we present such a generic result in Section 3.1, our main purpose is to outline some more intricate arguments, which use special properties of the congruence  $xy \equiv a \pmod{m}$  and cannot be generalised to other congruences. In particular, in Section 3.2 we discuss the behaviour of points on  $\mathcal{H}_{a,m}$  on average over  $a$ . We also describe some geometric properties of the set  $\mathcal{H}_{a,m}$  in Sections 4.1–4.3, show that it cannot be too concentrated even in very small squares in Section 4.4 and discuss some arithmetic properties of elements of  $\mathcal{H}_{a,m}$  in Section 4.5.

Before presenting results about the properties of  $\mathcal{H}_{a,m}$ , we give a short overview of the surprisingly diverse variety of number theoretic tools which have been used in the study of  $\mathcal{H}_{a,m}$  and their multivariate generalisations, see Sections 2.1–2.4.

Finally, we demonstrate the wealth and diversity of various applications of the results on the distribution of points on  $\mathcal{H}_{a,m}$ . Some of these applications are quite natural with very transparent connections to  $\mathcal{H}_{a,m}$ , see Section 5.1. However, there are also several less obvious and thus much more exciting applications, see Sections 5.2–5.20. An especially striking example of such unexpected applications is given by a result of [148] on torsions of elliptic curves, see Section 5.11.

### 1.3 Notation

Throughout the paper, any implied constants in symbols  $O$ ,  $\ll$  and  $\gg$  may occasionally depend, where obvious, on the real positive parameter  $\varepsilon$  and are absolute otherwise. We recall that the notations  $U = O(V)$ ,  $U \ll V$  and  $V \gg U$  are all equivalent to the statement that  $|U| \leq cV$  holds with some constant  $c > 0$ .

We use  $p$ , with or without a subscript, to denote a prime number and use  $m$  to denote a positive integer.

We denote by  $\mathbb{Z}/m\mathbb{Z}$  the residue ring modulo  $m$ . Typically we assume that the set  $\{0, \dots, m-1\}$  is used to represent the elements of  $\mathbb{Z}/m\mathbb{Z}$ . Accordingly, we often consider the following subset of  $\mathcal{H}_{a,m}$

$$\overline{\mathcal{H}}_{a,m} = \mathcal{H}_{a,m} \cap [0, m-1]^2.$$

We also put

$$\overline{\mathcal{H}}_m = \mathcal{H}_m \cap [0, m-1]^2.$$

We always follow the convention that arithmetic operations in the arguments of  $\mathbf{e}_m$  are performed modulo  $m$ . In particular, the Kloosterman sums (2) can also be written as

$$K_m(r, s) = \sum_{\substack{x=1 \\ \gcd(x,m)=1}}^m \mathbf{e}_m(rx + sx^{-1}).$$

As usual,  $\omega(k)$ ,  $\tau(k)$  and  $\varphi(k)$  denote the number of distinct prime divisors, the number of positive integer divisors and the Euler function of  $k \geq 1$ , respectively.

Finally,  $\mu(k)$  denotes the Möbius function. We recall that  $\mu(1) = 1$ ,  $\mu(k) = 0$  if  $k \geq 2$  is not squarefree and  $\mu(k) = (-1)^{\omega(k)}$  otherwise.

### 1.4 Acknowledgements

Thanks go to Mizan Khan who introduced the beautiful and mysterious world of modular hyperbolas to the author.

The author would also like to thank Alexey Ustinov, Arne Winterhof and the referee, for a careful reading of the manuscript and making many valuable suggestions.

This work was supported in part by ARC grant DP1092835.

## 2 Number Theory Background

### 2.1 Exponential and Character Sums

We have already mentioned the prominent role of Kloosterman sums (2) and the bound (1) in particular.

Most of the works also use the identity

$$\frac{1}{m} \sum_{r \in \mathbb{Z}/m\mathbb{Z}} \mathbf{e}_m(rv) = \begin{cases} 1, & \text{if } v \equiv 0 \pmod{m}, \\ 0, & \text{if } v \not\equiv 0 \pmod{m}, \end{cases} \quad (3)$$

to express various characteristic functions via exponential sums. Thus, we relate various counting questions to exponential sums.

It is very often complemented by the bound

$$\sum_{z=W+1}^{W+Z} \mathbf{e}_m(rz) \ll \min\{Z, m/|r|\} \quad (4)$$

which holds for any integers  $r$ ,  $W$  and  $Z \geq 1$  with  $0 < |r| \leq m/2$ , see [115, Bound (8.6)].

We now recall the estimate from [167] of exponential sums with rational functions of special type, which generalises the bound (1) of Kloosterman sums (2).

**Lemma 1.** *Let  $n_1, \dots, n_s$  be  $s \geq 2$  nonzero fixed pairwise distinct integers. Then the bound*

$$\max_{\gcd(a_1, \dots, a_s, m)=d} \left| \sum_{\substack{z=1 \\ \gcd(z, m)=1}}^m \mathbf{e}_m(a_1 z^{n_1} + \dots + a_s z^{n_s}) \right| \leq d^{1/s} m^{1-1/s+o(1)}$$

*holds.*

We recall that several more bounds of exponential sums with sparse polynomials of large degree are also given in [30, 33, 59].

However, in many cases using bounds of multiplicative character sums yields stronger results.

Let  $\Phi_m$  be the set of all  $\varphi(m)$  multiplicative characters modulo  $m$ . We have the following analogue of (3). For any integer  $r$ ,

$$\frac{1}{\varphi(m)} \sum_{\chi \in \Phi_m} \chi(r) = \begin{cases} 1 & \text{if } r \equiv 1 \pmod{m}, \\ 0 & \text{otherwise.} \end{cases} \quad (5)$$

We also use  $\chi_0$  to denote the principal character.

The following result is a combination of the Pólya-Vinogradov (for  $\nu = 1$ ) and Burgess (for  $\nu \geq 2$ ) bounds, see [115, Theorems 12.5 and 12.6].

**Lemma 2.** *For arbitrary integers  $W$  and  $Z$  with  $1 \leq Z \leq m$ , the bound*

$$\max_{\substack{\chi \in \Phi_m \\ \chi \neq \chi_0}} \left| \sum_{z=W+1}^{W+Z} \chi(z) \right| \leq Z^{1-1/\nu} m^{(\nu+1)/4\nu^2+o(1)}$$

*holds with  $\nu = 1, 2, 3$  for any  $m$  and with an arbitrary positive integer  $\nu$  if  $m = p$  is a prime.*

The identity (5) immediately implies that for  $1 \leq Z \leq m$

$$\sum_{\chi \in \Phi_m} \left| \sum_{z=W+1}^{W+Z} \chi(z) \right|^2 = \varphi(m) \sum_{\substack{z=W+1 \\ \gcd(z,m)=1}}^{W+Z} 1 \leq \varphi(m)Z \quad (6)$$

which has been used in many works on  $\mathcal{H}_{a,m}$ .

Furthermore, it turns out, that sometimes one gets better results using the following fourth moment estimate from [12] (for prime  $m = p$ ) and [83] (for arbitrary  $m$ ), see also [96]. In fact, these results have recently been generalised in [60], which we present in the following slightly less precise form.

**Lemma 3.** *For arbitrary integers  $W$ , and  $Z \leq m$ , the bound*

$$\sum_{\substack{\chi \in \Phi_m \\ \chi \neq \chi_0}} \left| \sum_{z=W+1}^{W+Z} \chi(z) \right|^4 \leq m^{1+o(1)} Z^2$$

*holds.*

Note that many of the results below are based on previous estimates of [12] (which require  $m = p$  to be prime) and [83] (which apply to any  $m$  but require  $W = 0$ ). So now Lemma 3 allows us to drop these restrictions.

For example, bounds of higher moments of multiplicative character sums, which in particular are based on combining Lemma 2 and a previous version of Lemma 3 with some other arguments, have been given [61], and can now be generalised.

In [93, 95] a new argument has been introduced to this area, which is based on a bound of [113] on the number of large values of Dirichlet polynomials, see also the original papers [114, 116] as well as [115, Chapter 9] for some other estimates for Dirichlet polynomials. This line of research is extremely interesting and definitely deserves more investigation.

## 2.2 Average Values of $L$ -functions

Many quantities related to the distribution of points on  $\mathcal{H}_{a,m}$  on average over  $a$ , lead to studying various average values of  $L$ -functions  $L(1, \chi)$  with multiplicative characters  $\chi \in \Phi_m$ , see, for example, [133, 134, 135, 136, 137, 143, 225]. Sometimes such sums are weighted by character sums and are of independent interest.

For example, let  $R_{a,m}(N)$  be the number of points  $(x, y) \in \mathcal{H}_{a,m}$  with  $1 \leq x \leq N$  and  $1 \leq y < m$ , and such that  $x + y$  is odd. It is shown in [143], that for a prime  $p$  the second moment of the differences  $R_{a,p}(N) - N/2$ ,  $a = 1, \dots, p-1$ , can be expressed via the sums

$$\begin{aligned}\sigma_1(p, N) &= \sum_{\substack{\chi \in \Phi_p \\ \chi(-1)=-1}} \left| \sum_{n=1}^N (-1)^n \chi(n) \right|^2 |L(1, \chi)|^2, \\ \sigma_2(p, N) &= \sum_{\substack{\chi \in \Phi_p \\ \chi(-1)=-1}} \chi(2) \left| \sum_{n=1}^N (-1)^n \chi(n) \right|^2 |L(1, \chi)|^2.\end{aligned}$$

Using a combination of the methods of [175, 226], in [143] the asymptotic formulas

$$\begin{aligned}\sigma_1(p, N) &= \alpha p N + O(N^2 p^{o(1)} + p(\log N)^2), \\ \sigma_2(p, N) &= \frac{\alpha}{2} p N + O(N^2 p^{o(1)} + p(\log N)^2).\end{aligned}$$

are given, where

$$\alpha = \frac{\pi^2}{12} \left( 1 + \frac{16}{9\zeta(3)} \sum_{k=1}^{\infty} \frac{1}{(2k+1)^2} \sum_{h=0}^k \frac{1}{2h+1} \right)$$

and  $\zeta(s)$  is the Riemann zeta-function. Clearly, the above formulas are non-trivial for  $p^\varepsilon < N \leq p^{1-\varepsilon}$  for any fixed  $\varepsilon > 0$ . On the other hand,

$$\sigma_1(p, p) = \sigma_2(p, p) = 0,$$

so there is some kind of the “phase-transition” area when  $N$  gets close to  $p$  which would be interesting to understand more.

## 2.3 Theory of Uniform Distribution

For a finite set  $\mathcal{F} \subseteq [0, 1]^s$  of the  $s$ -dimensional unit cube, we define its *discrepancy with respect to a domain*  $\Xi \subseteq [0, 1]^s$  as

$$\Delta(\mathcal{F}, \Xi) = \left| \frac{\#\{\mathbf{f} \in \mathcal{F} : \mathbf{f} \in \Xi\}}{\#\mathcal{F}} - \lambda(\Xi) \right|,$$

where  $\lambda$  is the Lebesgue measure on  $[0, 1]^s$ .

We now define the *discrepancy* of  $\mathcal{F}$  as

$$D(\mathcal{F}) = \sup_{\Pi \subseteq [0, 1]^s} \Delta(\mathcal{F}, \Pi),$$

where the supremum is taken over all boxes  $\Pi = [\alpha_1, \beta_1) \times \dots \times [\alpha_s, \beta_s) \subseteq [0, 1]^s$ .

A link between the discrepancy and exponential sums is provided by the celebrated *Koksma–Szűs inequality*, see [66, Theorem 1.21]. However, for points of  $\mathcal{H}_{a,m}$ , due to the discrete structure of the problem, one can immediately establish such a link directly by the identity (3).

For example, one can consider the points

$$\left(\frac{x}{m}, \frac{y}{m}\right) \in [0, 1]^2, \quad (x, y) \in \overline{\mathcal{H}}_{a,m},$$

and apply the bound (1) to estimate their discrepancy, which in turn is equivalent to studying points of  $\mathcal{H}_{a,m}(\mathcal{X}, \mathcal{Y})$  where  $\mathcal{X}$  and  $\mathcal{Y}$  are sets of consecutive integers.

Moreover, the *Koksma–Hlawka inequality*, see [66, Theorem 1.14], allows us to estimate average values of various functions on the points  $(x, y) \in \mathcal{H}_{a,m}$ .

**Lemma 4.** *For any continuous function  $\psi(\mathbf{z})$  on the unit cube  $[0, 1]^s$  and a finite set  $\mathcal{F} \subseteq [0, 1]^s$  of discrepancy  $D(\mathcal{F})$ , the following bound holds:*

$$\frac{1}{\#\mathcal{F}} \sum_{\mathbf{f} \in \mathcal{F}} \psi(\mathbf{f}) = \int_{[0, 1]^s} \psi(\mathbf{z}) d\mathbf{z} + O(D(\mathcal{F}))$$

where the implied constant depends only on  $s$  and the function  $\psi$ .



To study  $\mathcal{H}_{a,m} \cap \mathcal{W}$  for more general sets  $\mathcal{W}$  some additional tools are required from the theory of uniform distribution.

As usual, we define the distance between a vector  $\mathbf{u} \in [0, 1]^s$  and a set  $\Xi \subseteq [0, 1]^s$  by

$$\text{dist}(\mathbf{u}, \Xi) = \inf_{\mathbf{w} \in \Xi} \|\mathbf{u} - \mathbf{w}\|,$$

where  $\|\mathbf{v}\|$  denotes the Euclidean norm of  $\mathbf{v}$ . Given  $\varepsilon > 0$  and a domain  $\Xi \subseteq [0, 1]^s$  we define the sets

$$\Xi_\varepsilon^+ = \{\mathbf{u} \in [0, 1]^s \setminus \Xi : \text{dist}(\mathbf{u}, \Xi) < \varepsilon\}$$

and

$$\Xi_\varepsilon^- = \{\mathbf{u} \in \Xi : \text{dist}(\mathbf{u}, [0, 1]^s \setminus \Xi) < \varepsilon\}.$$

Let  $h(\varepsilon)$  be an arbitrary increasing function defined for  $\varepsilon > 0$  and such that

$$\lim_{\varepsilon \rightarrow 0} h(\varepsilon) = 0.$$

As in [128, 152], we define the class  $\mathcal{S}_h$  of domains  $\Xi \subseteq [0, 1]^s$  for which

$$\lambda(\Xi_\varepsilon^+) \leq h(\varepsilon) \quad \text{and} \quad \lambda(\Xi_\varepsilon^-) \leq h(\varepsilon)$$

for any  $\varepsilon > 0$ .

A relation between  $D(\mathcal{F})$  and  $\Delta(\mathcal{F}, \Xi)$  for  $\Xi \in \mathcal{S}_h$  is given by the following inequality of [128] (see also [152]).

**Lemma 5.** *For any domain  $\Xi \in \mathcal{S}_h$ , we have*

$$\Delta(\mathcal{F}, \Xi) \ll h(s^{1/2} D(\mathcal{F})^{1/s}).$$

Finally, the following bound, which is a special case of a more general result of H. Weyl [206] shows that if  $\Xi$  has a piecewise smooth boundary then  $\Xi \in \mathcal{S}_h$  for some linear function  $h(\varepsilon) = C\varepsilon$ .

**Lemma 6.** *For any domain  $\Xi \in [0, 1]^s$  with a piecewise smooth boundary, we have*

$$\lambda(\Xi_\varepsilon^\pm) = O(\varepsilon).$$

To use the above results for the study of points on  $\mathcal{H}_{a,m}$ , one usually considers points

$$\left(\frac{x}{m}, \frac{y}{m}\right) \in [0, 1]^2, \quad (x, y) \in \mathcal{H}_{a,m}, \quad 1 \leq x, y \leq m. \quad (7)$$

## 2.4 Arithmetic Functions, Divisors, Prime Numbers

Certainly some elementary bounds such as

$$\varphi(k) \gg \frac{k}{\log \log(k+2)}$$

and

$$2^{\omega(k)} \leq \tau(k) \leq \exp \left( (\log 2 + o(1)) \frac{\log k}{\log \log k} \right), \quad (8)$$

see [189, Section I.5.2 and I.5.4], appear at various stages of the proofs of relevant results.

The following well-known consequence of the *sieve of Eratosthenes* (essentially of the inclusion-exclusion principle expressed via the Möbius function) is very often needed to estimate the main terms of various asymptotic formulas (see, for example, [171, 176]).

**Lemma 7.** *For any integers  $m, Z \geq 1$  and  $W \geq 0$ ,*

$$\sum_{\substack{z=W+1 \\ \gcd(z,m)=1}}^{W+Z} 1 = \frac{\varphi(m)}{m} Z + O(2^{\omega(m)}).$$

For an infinite monotonically increasing sequence of positive integers  $\mathcal{A} = (a_n)_{n=1}^{\infty}$ , we define

$$H(x, y, z; \mathcal{A}) = \#\{n \leq x : \exists d|a_n \text{ with } y < d \leq z\}.$$

For  $\mathcal{A} = \mathbb{N}$ , the set of natural numbers, the order of magnitude of  $H(x, y, z; \mathbb{N})$  for all  $x, y, z$  has been determined in [73], see also [106]. Also in [73], one can find upper bounds for  $H(x, y, z; \mathcal{P}_b)$  of the expected order of magnitude, where  $\mathcal{P}_b = \{p+b : p \text{ prime}\}$  is a set of so-called shifted primes. However, for the problem of studying  $\mathcal{H}_{a,m}$ , we need analogous results where  $n$  is restricted to an arithmetic progression. More precisely, let us define the sequences

$$\mathcal{T}_k = \{mk - 1 : m \in \mathbb{N}\} \quad \text{and} \quad \mathcal{U}_k = \{pk - 1 : p \text{ prime}\}.$$

It has been shown in [75] that the arguments of [73] imply the following estimates.

It is usual that in questions of this kind, the constant

$$\kappa = 1 - \frac{1 + \log \log 2}{\log 2} = 0.086071 \dots \quad (9)$$

plays an important role, see also [106].

**Lemma 8.** *Uniformly for  $100 \leq y \leq x^{0.51}$ ,  $1.1y \leq z \leq y^{1.1}$ ,  $1 \leq k \leq \log x$ , we have*

$$\begin{aligned} H(x, y, z; \mathcal{T}_k) &\ll x \frac{k}{\varphi(k)} u^\kappa (\log(1/u))^{-3/2}, \\ H(x, y, z; \mathcal{U}_k) &\ll x \frac{k}{\varphi(k)} u^\kappa (\log(1/u))^{-3/2}, \end{aligned}$$

where  $z = y^{1+u}$ .

A certain result of [75] relies on the existence of infinitely many primes  $p$  with a prescribed structure of divisors of  $p - 1$ , which is done using a very deep result of [29] concerning the *Bombieri-Vinogradov theorem*.

For an integer  $k \geq 1$  we write

$$T(k) = \max_{i=1, \dots, \tau(k)-1} \frac{d_{i+1}}{d_i},$$

where  $1 = d_1 < \dots < d_{\tau(k)} = k$  are the positive divisors of  $k$ .

By [162, Theorem 1], we have:

**Lemma 9.** *Uniformly in  $z \geq t \geq 2$ ,*

$$\frac{z \log t}{\log z} \gg \# \{k \leq z : T(k) \leq t\} \gg \frac{z \log t}{\log z}.$$

Finally, we remark, that several interesting results about the distribution of points on  $\mathcal{H}_{a,m}(\mathcal{X}, \mathcal{Y})$  on average over  $a$ , for some special sets  $\mathcal{X}$  and  $\mathcal{Y}$ , such as intervals

$$\mathcal{X} = \mathcal{Y} = \{z : 1 \leq z \leq m/2\},$$

are based on various asymptotic formulas for average values of Dirichlet  $L$ -functions, see, for example, [133, 210, 225].

## 2.5 Integer Points on Algebraic Surfaces and Convex Polygons

The result of [125, Theorem 2] is based on the following bound on the number of solutions to a bivariate quadratic Diophantine equation, which follows from [201, Lemma 3.5] combined with [51, Proposition 1] and [166, Theorem 1]:

**Lemma 10.** *Let*

$$G(X, Y) = AX^2 + BXY + CY^2 + DX + EY + F \in \mathbb{Z}[X, Y]$$

*be an irreducible quadratic polynomial with coefficients of size at most  $H$ . Assume that  $G(X, Y)$  is not affine equivalent to a parabola  $Y = X^2$  and has a nonzero determinant*

$$\Delta = B^2 - 4AC \neq 0.$$

*Then the equation  $G(x, y) = 0$  has at most  $H^{o(1)}$  integral solutions  $(x, y) \in [0, H] \times [0, H]$ .*

As usual, we say that a polygon  $\mathcal{P} \subseteq \mathbb{R}^2$  is integral if all its vertices belong to the integral lattice  $\mathbb{Z}^2$ .

Also, following [8] we say two polygons  $\mathcal{P}, \mathcal{Q} \subseteq \mathbb{R}^2$  are equivalent if there is an affine transformation

$$T : \mathbf{x} \mapsto A\mathbf{x} + \mathbf{b}, \quad \mathbf{x} \in \mathbb{R}^2,$$

for  $A = \text{GL}_2(\mathbb{Z})$  and  $\mathbf{b} \in \mathbb{Z}^2$  preserving the integral lattice  $\mathbb{Z}^2$  (that is,  $\det A = \pm 1$ ) that maps  $\mathcal{P}$  to  $\mathcal{Q}$ .

The following result of [16, Lemma 3] plays an important role in the argument of [125]

**Lemma 11.** *An integral polygon of area  $S$  is equivalent to a polygon contained in some box  $[0, u] \times [0, v]$  of area  $uv \leq 4S$ .*

Besides, the approach of [125] also makes use a special case of the following general result of [153, Lemma 2.2] which we use only in  $\mathbb{R}^2$ .

**Lemma 12.** *Let  $\mathfrak{U} \subseteq \mathbb{R}^d$  be a convex compact. We consider a finite sequence of compacts  $\mathfrak{V}_i \subseteq K$ ,  $i = 1, \dots, n$ , such that none of them meets the convex hull of others. Then*

$$\sum_{i=1}^n (\text{vol } \mathfrak{V}_i)^{(d-1)/(d+1)} \ll (\text{vol } \mathfrak{U})^{(d-1)/(d+1)},$$

*where  $\text{vol } \mathfrak{A}$  denotes the volume of a compact set  $\mathfrak{A} \subseteq \mathbb{R}^d$  and the implied constant depends only on  $d$ .*

Furthermore, a result of [74] (that has been improved in [125]) uses the bound  $O(S^{1/3})$  of [7] on the number of integer vertices of a convex polygon of area  $S$ .

### 3 Distribution of Points on $\mathcal{H}_{a,m}$

#### 3.1 Points on $\mathcal{H}_{a,m}$ in Intervals for All $a$

A classical conjecture asserts that for any fixed  $\varepsilon > 0$  and a sufficiently large  $p$ , for every integer  $a$  there are integers  $x$  and  $y$  with  $|x|, |y| \leq p^{1/2+\varepsilon}$  such that  $xy \equiv a \pmod{p}$ ; see [91, 97, 98, 99] and references therein. The question has probably been motivated by the following observation. Using the Dirichlet pigeon-hole principle, one can easily show that for every integer  $a$  there are integers  $x$  and  $y$  with  $|x|, |y| \leq p^{1/2}$  and  $x/y \equiv a \pmod{p}$ .

Unfortunately, this is known only with  $|x|, |y| \leq Cp^{3/4}$  for some absolute constant  $C > 0$ , which is shown in [92]. Several modifications of this bound, for example for composite  $m$ , are also known, see [123]. These results are based on the bound (1) of Kloosterman sums (2) (and its more precise form in the case when  $m = p$  is a prime) combined with some other standard arguments. The same arguments also produce the following estimate which is a slight generalisation of several previously known results, see [17, 88] and references therein. This estimate is certainly very well-known and has appeared in the literature in various forms. We however give a short proof in order to demonstrate the underlying techniques.

**Theorem 13.** *Let  $\mathcal{X} = \{U + 1, \dots, U + X\}$ , where  $m > X \geq 1$  and  $U \geq 0$  are arbitrary integers. Suppose that for every  $x \in \mathcal{X}$  we are given a set  $\mathcal{Y}_x = \{V_x + 1, \dots, V_x + Y\}$  where  $m > Y \geq 1$  and  $V_x \geq 0$  are arbitrary integers. Then for any integer  $m \geq 1$  and  $a$  with  $\gcd(a, m) = 1$ , we have*

$$\sum_{\substack{(x,y) \in \mathcal{H}_{a,m} \\ x \in \mathcal{X}, y \in \mathcal{Y}_x}} 1 = \frac{\varphi(m)}{m^2} XY + O(m^{1/2+o(1)}).$$

*Proof.* Using (3) we write

$$\begin{aligned} \sum_{\substack{(x,y) \in \mathcal{H}_{a,m} \\ x \in \mathcal{X}, y \in \mathcal{Y}_x}} 1 &= \frac{1}{m^2} \sum_{\substack{(x,y) \in \mathcal{H}_{a,m} \\ 1 \leq x, y \leq m}} \sum_{w \in \mathcal{X}} \sum_{z \in \mathcal{Y}_w} \sum_{r, s \in \mathbb{Z}/m\mathbb{Z}} \mathbf{e}_m(r(x-w) + s(y-z)) \\ &= \frac{1}{m^2} \sum_{r, s \in \mathbb{Z}/m\mathbb{Z}} K_m(r, as) \sum_{w \in \mathcal{X}} \mathbf{e}_m(-rw) \sum_{z \in \mathcal{Y}_w} \mathbf{e}_m(-sz). \end{aligned}$$

We now separate the main term which corresponds to  $r = s = 0$  and is equal

to

$$\frac{XY}{m^2} \sum_{\substack{(x,y) \in \mathcal{H}_{a,m} \\ 1 \leq x,y \leq m}} 1 = \frac{\varphi(m)}{m^2} XY.$$

For the error term  $\mathbf{E}$ , for each divisor  $d|m$ , we collect together pairs  $(r, s)$  with the same value  $\gcd(r, s, m) = d$ .

Applying the bounds (1) and (4) we obtain

$$\begin{aligned} |\mathbf{E}| &\leq m^{1/2+o(1)} \sum_{\substack{d|m \\ d < m}} d^{1/2} \sum_{\substack{-(m-1)/2 \leq r, s \leq m/2 \\ \gcd(r, s, m) = d}} \frac{1}{(|r| + 1)(|s| + 1)} \\ &\leq m^{1/2+o(1)} \sum_{\substack{d|m \\ d < m}} d^{1/2} \left( \sum_{|t| \leq m/2d} \frac{1}{d|t| + 1} \right)^2 \\ &\leq m^{1/2+o(1)} \sum_{\substack{d|m \\ d < m}} d^{-3/2} \leq m^{1/2+o(1)}, \end{aligned}$$

which leads to the desired statement.  $\square$

For example if  $V_x = V$  for all  $x \in \mathcal{X} = \{U + 1, \dots, U + X\}$  and  $\mathcal{Y} = \{V + 1, \dots, V + Y\}$  then Theorem 13 yields

$$\#\mathcal{H}_{a,m}(\mathcal{X}, \mathcal{Y}) = \frac{\varphi(m)}{m^2} XY + O(m^{1/2+o(1)}). \quad (10)$$

It seems that improving Theorem 13 or even just the asymptotic formula (10) and making them nontrivial for  $XY < m^\alpha$  with some fixed  $\alpha < 3/2$  is out of reach at the present time. In particular, this exponent is related to the fact that an asymptotic formula for the sum of  $\tau(n)$  for integers  $n \leq X$  in an arithmetic progression  $n \equiv a \pmod{m}$  is known only for  $m \leq X^{2/3-\varepsilon}$  for an arbitrary fixed  $\varepsilon > 0$ . This result has been independently discovered by A. Selberg and C. Hooley (see, for example, the discussion in [110]) and has resisted any improvement for more than half a century.

In turn, any improvement of Theorem 13 or just of (10) will trigger a chain reaction of improvements in many other problems; in particular some of them are outlined in this survey. Probably the most feasible way to tackle

this problem is to obtain good bounds of incomplete Kloosterman sums, improving the estimate

$$\left| \sum_{\substack{V+1 \leq x \leq V+X \\ \gcd(x, m)=1}} \mathbf{e}_m(sx^{-1}) \right| \leq (m \gcd(s, m))^{1/2+o(1)}, \quad 1 \leq X \leq m,$$

which is immediate from (1). We recall that a famous conjecture of Hoo-ley [111] asserts that if  $\gcd(s, m) = 1$  then the bound

$$\left| \sum_{\substack{1 \leq x \leq X \\ \gcd(x, m)=1}} \mathbf{e}_m(sx^{-1}) \right| \leq X^{1/2} m^{o(1)}, \quad (11)$$

holds uniformly over  $m^{1/4} \leq X \leq m$ . The conjectured bound (11) enables us to derive that for  $\mathcal{X} = \{1, \dots, X\}$  with  $X \geq m^{1/4}$  and  $\mathcal{Y} = \{V+1, \dots, V+Y\}$  we have

$$\#\mathcal{H}_{a,m}(\mathcal{X}, \mathcal{Y}) = \frac{\varphi(m)}{m^2} XY + O(X^{1/2} m^{o(1)}).$$

For example, we see that assuming (11) one can show that for any  $\varepsilon$  and sufficiently large prime  $p$ , for every integer  $a$  there are integers  $x$  and  $y$  with  $|x|, |y| \leq p^{2/3+\varepsilon}$  and such that  $xy \equiv a \pmod{p}$ . Unfortunately, the conjecture (11) seems to be extremely difficult; see however [126] for some improvements of the bound (1).

On the other hand, there are some apparently easier questions which could be more feasible to answer.

**Question 14.** *Improve the asymptotic formula (10) for some special moduli  $m$ , such as primes or prime powers.*

It is quite possible that the method and results of [76] can be use to give a positive answer to the next problem; see [74] where the results of [76] have been used to study the distribution of points on  $\mathcal{H}_{a,m}$ .

**Question 15.** *Improve the asymptotic formula (10) on average over the moduli  $m \leq M$ .*

Clearly, Theorem 13 can be viewed as the bound  $O(m^{-1/2+o(1)})$  on the discrepancy of the points (7). Thus one can now apply Lemmas 5 and (6) to study the distribution of points on  $\mathcal{H}_{a,m}$  in more complicated domains than boxes  $[U+1, U+X] \times [V+1, V+Y]$  covered by Theorem 13. For example, we immediately deduce that

$$\#\{(x, y) \in \overline{\mathcal{H}}_{a,m} : x^2 + y^2 \leq r^2\} = \frac{\pi r^2 \varphi(m)}{4m^2} + O(m^{3/4+o(1)}).$$

Furthermore, the asymptotic formula (10), combined with Lemma 4, provides the most direct way to the following asymptotic formula

$$\sum_{(x,y) \in \overline{\mathcal{H}}_{a,m}} (x-y)^{2\nu} = \frac{1}{(2\nu+1)(\nu+1)} m^{2\nu} \varphi(m) + O(m^{2\nu+1/2+o(1)}) \quad (12)$$

which has been given in [221] (in a slightly more precise form, which can also be obtained within our elementary arguments).

Similarly Theorem 13 and Lemma 4 imply that for any real positive  $\Delta < m/2$

$$\sum_{\substack{(x,y) \in \overline{\mathcal{H}}_{a,m} \\ |x-y| \leq \Delta}} 1 = \frac{\Delta(2m-\Delta)\varphi(m)}{m^2} + O(m^{1/2+o(1)}) \quad (13)$$

which is a version of a result of [222].

As we have mentioned, Theorem 13 uses very little specific information about the congruence  $xy \equiv a \pmod{m}$  and can be extended to many other congruences. For prime  $m = p$  one can use the Bombieri bound [28] instead of (1) and obtain exactly the same results in much more general settings. For example, this has been done for solutions of polynomial congruences modulo  $p$  and also for joint distribution of inverses modulo  $p$  of  $s$  linear forms  $a_j x + b_j$ ,  $j = 1, \dots, s$ , with integer coefficients, see [45, 53, 55, 56, 57, 58, 103, 200, 215, 224, 228, 229] and references therein.

We also remark a very nice and completely elementary result of [48] about the distances between inverses on pairs of consecutive integers.

It is also easy to use some other bounds of more general exponential sums (instead of (1)) to study the distribution of values of polynomials and rational functions on the points of  $\mathcal{H}_{a,m}$ .

For example, in [212, 224] some questions are studied about the distribution of residues modulo  $m$  of powers  $(x^k, y^k)$  taken over all  $(x, y) \in \overline{\mathcal{H}}_{a,m}$ . In



particular, it has been shown in [212], that for any fixed integer  $k \neq 0$ , the smallest positive residue modulo  $m$  of  $n^k$  and its modular inverse  $\overline{n^k}$  are of the same parity

$$N(k, m) = 0.5\varphi(m) + O(m^{3/4+o(1)}) \quad (14)$$

times when  $n$  runs through all invertible elements of  $\mathbb{Z}/m\mathbb{Z}$ .

These results can be substantially extended and improved if one uses Lemma 1. In particular, it has been shown in [174] that Lemma 1 immediately implies that the error term can be lowered from  $m^{3/4+o(1)}$  to  $m^{1/2+o(1)}$  in (14), that is, we have

$$N(k, m) = 0.5\varphi(m) + O(m^{1/2+o(1)}).$$

Moreover, it is shown in [174] that an analogous asymptotic formula (with the error term  $m^{1-1/s+o(1)}$ ) for the counting function of the number of residues of  $s$  distinct powers  $x^{k_1}, \dots, x^{k_s}$ , where  $k_1, \dots, k_s \in \mathbb{Z} \setminus \{0\}$ , of  $x$  modulo  $m$  which belong to  $s$  prescribed arithmetic progressions. All these results can be obtained by combining Lemma 1 with standard arguments similar to those used in the proof of Theorem 13.

In [41, 194] one can find asymptotic formulas for the number of points of  $(x, y) \in \mathcal{H}_{a,m}$  in more complicated regions of the form

$$x \in \{U + 1, \dots, U + X\}, \quad 0 \leq y \leq f(x), \quad (15)$$

where  $f(t)$  is a twice differentiable function which satisfies

$$F \ll |f''(t)| \ll F, \quad t \in [U + 1, U + X],$$

for some  $F \geq 1$  (the error term also involves  $F$ ). It is shown in [41] that this question has applications to sums of divisor function with quadratic polynomials. Further investigations in this directions would be of great interest.

### 3.2 Points on $\mathcal{H}_{a,m}$ in Intervals on Average Over $a$

It is natural to expect that one can get stronger results than Theorem 13 on average over  $a$ .

This indeed is true, and it has been shown in the series of works [91, 97, 98, 99] that the congruence  $a \equiv xy \pmod{m}$  is solvable for all but  $o(m)$  values of  $a = 1, \dots, m - 1$ , with  $x$  and  $y$  significantly smaller than  $m^{3/4}$ . In particular, in [98], this is proved for  $x$  and  $y$  in the range  $1 \leq x, y \leq$

$m^{1/2}(\log m)^{1+\varepsilon}$ . Certainly this result is very sharp. Indeed, it has been noticed in [91] that well-known estimates for integers with a divisor in a given interval (see [73, 106]) immediately imply that for any  $\varepsilon > 0$  almost all residue classes modulo  $m$  are not of the form  $xy \pmod{m}$  with  $1 \leq x, y \leq m^{1/2}(\log m)^{\kappa-\varepsilon}$  where  $\kappa$  is given by (9).

One can also derive from [75] (which in turn makes use of Lemma 8) that for any  $\varepsilon > 0$  the inequality

$$\max\{|x|, |y| : xy \equiv 1 \pmod{m}\} \geq m^{1/2}(\log m)^{\kappa/2}(\log \log m)^{3/4-\varepsilon}$$

holds:

- for all positive integers  $m \leq M$ , except for possibly  $o(M)$  of them,
- for all prime  $m = p \leq M$  except for possibly  $o(M/\log M)$  of them.

In [74], some ideas and results of [76] have been used to show that

$$\max\{|x|, |y| : xy \equiv 1 \pmod{m}\} \leq m^{1/2+o(1)}$$

for all positive integers  $m \leq M$ , except for possibly  $o(M)$  of them. So this implies that the above estimates of [75] are quite tight and also settles a slightly relaxed form of one of the conjectures of [75].

Similar questions about the ratios  $x/y$ , have also been studied, see [91, 98, 164].

The result of [98] shows that almost all reduced classes modulo  $m$  can be represented as  $xy$  with  $1 \leq x, y \leq m^{1/2+\varepsilon}$ . However, it does not imply that these products are uniformly distributed in reduced residue classes, which is sometimes required in applications.

In this respect, the following bound is a minor modification of a result of [171] and gives the desired uniformity of distribution for  $1 \leq x \leq X$ ,  $V+1 \leq y \leq V+Y$  provided that  $X, Y \geq m^{1/2+\varepsilon}$  for a fixed  $\varepsilon > 0$  and sufficiently large integer  $m$ . In turn, it is based on some ideas from [15].

**Theorem 16.** *Let  $\mathcal{X} = \{1, \dots, X\}$  and  $\mathcal{Y} = \{V+1, \dots, V+Y\}$  where  $X, Y \geq 1$  and  $V \geq 0$  are arbitrary integers. Then for any integer  $m \geq 1$ ,*

$$\sum_{\substack{a=1 \\ \gcd(a,m)=1}}^m \left| \#\mathcal{H}_{a,m}(\mathcal{X}, \mathcal{Y}) - \frac{\varphi(m)}{m^2}XY \right|^2 \leq X(X+Y)m^{o(1)}.$$

*Proof.* We rewrite the congruence  $xy \equiv a \pmod{m}$  as  $y \equiv ax^{-1} \pmod{m}$  (where the inversion is taken modulo  $m$ ). Using the identity (3), we write

$$\begin{aligned} \#\mathcal{H}_{a,m}(\mathcal{X}, \mathcal{Y}) &= \frac{1}{m} \sum_{\substack{x=1 \\ \gcd(x,m)=1}}^X \sum_{y=V+1}^{V+Y} \sum_{-(m-1)/2 \leq r \leq m/2} \mathbf{e}_m(r(ax^{-1} - y)) \\ &= \frac{1}{m} \sum_{-(m-1)/2 \leq r \leq m/2} \mathbf{e}_m(-rV) \sum_{\substack{x=1 \\ \gcd(x,m)=1}}^X \mathbf{e}_m(arx^{-1}) \sum_{y=1}^Y \mathbf{e}_m(-ry). \end{aligned}$$

By Lemma 7, the main term corresponding to  $r = 0$  is

$$\frac{1}{m} \sum_{\substack{x=1 \\ \gcd(x,m)=1}}^X \sum_{y=1}^Y 1 = \frac{\varphi(m)}{m^2} XY + O(Ym^{-1+o(1)}).$$

Hence

$$\#\mathcal{H}_{a,m}(\mathcal{X}, \mathcal{Y}) - \frac{\varphi(m)}{m^2} XY \ll \frac{1}{m} |\mathbf{E}_{a,m}(X, Y)| + Ym^{-1+o(1)},$$

where

$$\mathbf{E}_{a,m}(X, Y) = \sum_{1 \leq |r| \leq m/2} \sum_{\substack{x=1 \\ \gcd(x,m)=1}}^X \mathbf{e}_m(arx^{-1}) \sum_{y=1}^Y \mathbf{e}_m(-ry).$$

Using the Cauchy inequality (and the extending the summation to all residue classes modulo  $m$ ), we derive

$$\begin{aligned} \sum_{\substack{a=1 \\ \gcd(a,m)=1}}^m \left| \#\mathcal{H}_{a,m}(\mathcal{X}, \mathcal{Y}) - \frac{\varphi(m)}{m^2} XY \right|^2 \\ \ll \frac{1}{m^2} \sum_{a=1}^m |\mathbf{E}_{a,m}(X, Y)|^2 + Y^2 m^{-1+o(1)}. \end{aligned} \tag{16}$$

We now put  $J = \lfloor \log(Y/2) \rfloor$  and define the sets

$$\begin{aligned} \mathcal{R}_0 &= \left\{ r : 1 \leq |r| \leq \frac{m}{Y} \right\}, \\ \mathcal{R}_j &= \left\{ r : e^{j-1} \frac{m}{Y} < |r| \leq e^j \frac{m}{Y} \right\}, \quad j = 1, \dots, J, \\ \mathcal{R}_{J+1} &= \left\{ r : e^J \frac{m}{Y} < |r| \leq m/2 \right\} \end{aligned}$$

(we can certainly assume that  $J \geq 1$  since otherwise the bound is trivial).

Applying the Cauchy inequality again, we deduce

$$|\mathbf{E}_{a,m}(X, Y)|^2 \leq (J+2) \sum_{j=0}^{J+1} |\mathbf{E}_{a,m,j}(X, Y)|^2, \quad (17)$$

where

$$\mathbf{E}_{a,m,j}(X, Y) = \sum_{r \in \mathcal{R}_j} \sum_{\substack{x=1 \\ \gcd(x,m)=1}}^X \mathbf{e}_m(arx^{-1}) \sum_{y=1}^Y \mathbf{e}_m(-ry).$$

Using (4), we conclude that

$$\sum_{y=1}^Y \mathbf{e}_m(-ry) \ll e^{-j} Y.$$

for  $r \in \mathcal{R}_j$ ,  $j = 0, \dots, J+1$ . Thus

$$\mathbf{E}_{a,m,j}(X, Y) \ll e^{-j} Y \left| \sum_{r \in \mathcal{R}_j} \vartheta_r \sum_{\substack{x=1 \\ \gcd(x,m)=1}}^X \mathbf{e}_m(arx^{-1}) \right|, \quad j = 0, \dots, J+1,$$

for some complex numbers  $\vartheta_r$  with  $|\vartheta_r| \leq 1$  for  $|r| \leq m/2$ . Therefore,

$$\begin{aligned} \sum_{a=1}^m |\mathbf{E}_{a,m,j}(X, Y)|^2 &\ll e^{-2j} Y^2 \sum_{a=1}^m \left| \sum_{r \in \mathcal{R}_j} \vartheta_r \sum_{\substack{x=1 \\ \gcd(x,m)=1}}^X \mathbf{e}_m(arx^{-1}) \right|^2 \\ &= e^{-2j} Y^2 \sum_{r_1, r_2 \in \mathcal{R}_j} \vartheta_{r_1} \vartheta_{r_2} \sum_{\substack{x_1, x_2 \leq X \\ \gcd(x_1 x_2, m)=1}}^X \sum_{a=1}^m \mathbf{e}_m(a(r_1 x_1^{-1} - r_2 x_2^{-1})). \end{aligned}$$

Clearly the inner sum vanishes if  $r_1 x_1^{-1} \not\equiv r_2 x_2^{-1} \pmod{m}$  and is equal to  $m$  otherwise. Therefore

$$\sum_{a=1}^m |\mathbf{E}_{a,m,j}(X, Y)|^2 \ll e^{-2j} Y^2 m T_j, \quad (18)$$

where  $T_j$  is the number of solutions to the congruence

$$r_1 x_2 \equiv r_2 x_1 \pmod{m}, \quad r_1, r_2 \in \mathcal{R}_j, \quad x_1, x_2 \leq X, \quad \gcd(x_1 x_2, m) = 1.$$

We now see that if  $r_1$  and  $x_2$  are fixed, then  $r_2$  and  $x_1$  are such that their product  $s = r_2 x_1 \ll e^j m X / Y$  belongs to a prescribed residue class modulo  $m$ . Thus there are at most  $O(e^j X / Y + 1)$  possible values of  $s$  and for each fixed  $s \ll e^j m X / Y$  there are  $\tau(s) = m^{o(1)}$  values of  $r_1$  and  $x_2$  with  $s = r_1 x_2$ , see (8). Therefore

$$T_j \leq X \# \mathcal{R}_j (e^j X / Y + 1) m^{o(1)} = \frac{e^{2j} X^2 m^{1+o(1)}}{Y^2} + \frac{e^j X m^{1+o(1)}}{Y}$$

and after substitution into (18) we get

$$\sum_{a=1}^m |\mathbf{E}_{a,m,j}(X, Y)|^2 \ll e^{-2j} Y^2 m T_j = X^2 m^{2+o(1)} + e^{-j} X Y m^{2+o(1)}.$$

Substituting this bound in (17) and recalling (16), we conclude the proof.  $\square$

We note that the proof of Theorem 16 can easily be extended to arbitrary sets  $\mathcal{X} \subseteq \{1, \dots, X\}$ , see [171]. However, it breaks down if  $x$  runs through a short interval away from the origin. An alternative approach has been suggested in [96] and is based on bounds of the fourth moment of multiplicative character sums, see Lemma 3. If  $m = p$  is prime, it can handle such shifted intervals  $\mathcal{X} = \{U + 1, \dots, U + X\}$  (but not arbitrary sets  $\mathcal{X} \subseteq \{1, \dots, X\}$  as that of [171]). Furthermore, the technique of [96] leads to more explicit expressions instead of  $m^{o(1)}$  in the error term. Thus, although the approaches of [96] and [171] complement each other they still leave some natural open questions.

**Question 17.** *Extend Theorem 16 to sets  $\mathcal{X} = \{U + 1, \dots, U + X\}$  with arbitrary  $U$ .*

As we have mentioned, if  $m = p$ , Question 17 is addressed in [96], however some of the necessary ingredients are not known for composite  $m$ .

In [49] the behaviour of  $\# \mathcal{H}_{a,m}(\mathcal{X}, \mathcal{Y})$  has been studied for the sets  $\mathcal{X} = \{U + 1, \dots, U + X\}$  and  $\mathcal{Y} = \{V + 1, \dots, V + Y\}$  on average over  $U$  and  $V$ . It is shown in [49] that  $\# \mathcal{H}_{a,m}(\mathcal{X}, \mathcal{Y})$  is close to its expected value  $XY \varphi(m) / m^2$  for almost all  $U, V \in \mathbb{Z}_m$  provided that  $X, Y \geq m^{1/2+\varepsilon}$  for some fixed  $\varepsilon > 0$ . Furthermore, one can also find in [49] a similar statement for a multidimensional analogues of  $\# \mathcal{H}_{a,m}(\mathcal{X}, \mathcal{Y})$ . Several more results of this kind have been given in [100], however in the setting of [100] the initial point of only one interval is “sliding”, while the other one is fixed, see also [40].

We also note that several results “on average” related to various modifications of the *Lehmer problem* are given in [133, 205, 209, 210, 211, 214, 216, 225, 227], see also Section 5.1.

Finally, we remark that  $\#\mathcal{H}_{a,m}(\mathcal{X}, \mathcal{Y})$  has been studied in [54] for the same sets as in Theorem 13, that is, for  $\mathcal{X} = \{1, \dots, X\}$  and  $\mathcal{Y} = \{V + 1, \dots, V + Y\}$ , but on average over  $V$ . It is shown in [54] that in this case one can also obtain stronger bounds than that of Theorem 13.

### 3.3 Points on $\mathcal{H}_{a,m}$ in Sets with Arithmetic Conditions

Theorems 13 and 16 consider the case when  $x$  and  $y$  belong to sets of consecutive integers. However, studying points on  $\mathcal{H}_{a,m}$  in other sets is of ultimate interest as well.

We start with a very simple observation that no general result of the type of Theorems 13 and 16 applying to arbitrary sets  $\mathcal{X}$  and  $\mathcal{Y}$  is possible (even for very massive sets  $\mathcal{X}$  and  $\mathcal{Y}$ ). For example, if  $m = p$  is a prime and  $\mathcal{X} = \mathcal{Y}$  consist of all  $(p-1)/2$  quadratic residues modulo  $p$ , then  $\mathcal{H}_{a,p}(\mathcal{X}, \mathcal{Y}) = \emptyset$  for every quadratic nonresidue  $a$ .

The problem of distribution of pairs of primes  $(p, q) \in \overline{\mathcal{H}}_{a,m}$  has been considered in [71]. Unfortunately, it seems that even the *Extended Riemann Hypothesis* is not powerful enough to get a satisfactory answer to this question, see [71] for details. However, on average over both  $a$  and  $m$  this problem becomes more feasible and has actually been considered in [84]. More precisely, let  $P(X; m, a)$  be the number of solutions to the congruence

$$p_1 p_2 \equiv a \pmod{m}$$

in primes  $p_1, p_2 \leq X$ . It is shown in [84] that for any sufficiently large  $M$ ,

$$\sum_{M < m \leq 2M} \sum_{\substack{a=1 \\ \gcd(a,m)=1}}^m \left( P(X; m, a) - \frac{\pi(X)^2}{\varphi(m)} \right)^2 \ll X^4 (\log X)^{-A} + MX^2,$$

for any  $A$ , with an implied constant that depends on  $A$ , and

$$\sum_{M < p \leq 2M} \sum_{a=1}^{p-1} \left( P(X; p, a) - \frac{\pi(X)^2}{p-1} \right)^2 \ll (M^{-1}X^4 + MX^2) (\log X)^{-2}.$$

The number  $S(X; m, a)$  of solutions to the congruence

$$s_1 s_2 \equiv a \pmod{m}$$

in squarefree positive integers  $s_1, s_2 \leq X$  is certainly easier to study and in this case “individual” results are possible. For example, it is shown in [84] that for all integers  $m \geq 1$  and  $a$  with  $\gcd(a, m) = 1$  and real positive  $x$ , we have

$$S(X; m, a) = \frac{36}{\pi^4} \cdot \frac{X^2}{m} \prod_{p|m} \left(1 + \frac{1}{p} - \frac{1}{p^2} + \frac{1}{p^3}\right)^{-1} + O(Xm^{-1/4+o(1)}). \quad (19)$$

Moreover, representations of residue classes by products of a squarefree number and a prime have also been studied [84] (for a fixed modulus but on average over residue classes).

The result of [86] on the distribution of values of the Euler function in residues classes is based on studying congruences with products of shifted primes

$$(p_1 - 1)(p_2 - 1)(p_3 - 1) \equiv a \pmod{m}$$

and employing bounds of multiplicative character sums with shifted primes from [117, 154]; see also [85] for some related results on some residue classes modulo  $m$  which are “hard” to represent by a totient.

In [93] an improvement of some results of [86] has been obtained. This new idea of [93] is to use a bound of [113] on the number of large values of Dirichlet polynomials (see also [115, Chapter 9]), and can probably be applied to a number of other questions. For example, one of such applications to the distribution of points on multivariate modular hyperbolas is given in [95].

It is shown in [84] that there are two absolute constants  $\eta, \kappa > 0$  such that for any prime  $p$  and integer  $X$  with  $p > X \geq p^{1-\eta}$ , if  $\gcd(ak, p) = 1$  then the congruence

$$p_1 p_2 (p_3 + k) \equiv a \pmod{p}$$

has  $(1 + O(p^{-\kappa}))\pi(X)^3/p$  solutions in primes  $p_1, p_2, p_3 \leq X$  (uniformly over  $a$  and  $k$ ). It is shown in [95], using a result of [113], that one can take any  $\eta < 13/76$ .

In [94], for  $X \leq p$ , the bound

$$\max_{\gcd(b,p)=1} \left| \sum_{\substack{q \leq X \\ q \text{ prime}}} \mathbf{e}_p(bq^{-1}) \right| \ll (X^{15/16} + X^{2/3}p^{1/4}) p^{o(1)} \quad (20)$$

has been obtained for exponential sums of reciprocals of primes, which is in this special case an improvement of a more general result of [79]. In turn, this has led to an improvement of the result of [84] for the number of solutions of the congruence

$$p_1(p_2 + p_3) \equiv a \pmod{p} \quad (21)$$

in primes  $p_1, p_2, p_3 \leq X$ . More precisely, in [94], the asymptotic formula  $(1 + O(p^{-\kappa}))\pi(X)^3/p$  for the number of solutions is shown to hold for  $p \geq X \geq p^{16/17+\varepsilon}$ , where  $\kappa > 0$  depends only on  $\varepsilon > 0$ . Note that the exponent  $16/17$  improves the previous exponent  $38/39$  of [84] that is based on the estimate of [79]. Using the bound of [80] on the average values of such exponential sums

$$\sum_{Z \leq p \leq 2Z} \max_{\gcd(b,p)=1} \left| \sum_{\substack{q \leq X \\ q \text{ prime}}} \mathbf{e}_p(bq^{-1}) \right| \ll (X^{3/5} Z^{13/10} + X^{5/6} Z^{13/12}) Z^{o(1)}, \quad (22)$$

where  $X \leq Z$ , for almost all primes  $p$ , one can obtain a similar result for  $p \geq X \geq p^{13/14+\varepsilon}$ . We note that the both bounds (20) and (22) are nontrivial for  $X \geq p^{3/4+\varepsilon}$  for some fixed  $\varepsilon > 0$ . The bound of [31, Theorem 4.1] is nontrivial for  $X \geq p^{1/2+\varepsilon}$ , however it is less explicit. Recently, an explicit version of the results of [31] has been given in [14] how it is not immediately clear whether it can lead to new results about the congruence (21) (except for the case where the variables are in the domain  $p_1 \leq X$ ,  $p_2, p_3 \leq Y$  with  $X$  substantially smaller than  $Y$ ).

Furthermore, yet another approximation to the initial problem has been considered in [180]. Combining a generalisation of the bound (20) to composite denominators (given in [80]) with the sieve method, it is shown in [180] that for a sufficiently large  $m$  and any  $a$  with  $\gcd(a, m) = 1$  there is a solution to the congruence

$$pP_{17} \equiv a \pmod{m}, \quad p, P_{17} \leq m^{0.997},$$

where  $p$  is prime and  $P_{17}$  has at most 17 prime divisors.

One can also study the distribution of points  $(x, y) \in \mathcal{H}_{a,m}(\mathcal{X}, \mathcal{Y})$  with some prescribed structure of prime factors. For example, let  $P_+(k)$  and  $P_-(k)$  denote the largest and the smallest prime divisors of an integer  $k \geq 1$ , respectively.



**Question 18.** *Obtain an asymptotic formula for*

$$\#\{(x, y) \in \mathcal{H}_{a,m}(\mathcal{X}, \mathcal{Y}) : P_+(xy) \leq R\}$$

and

$$\#\{(x, y) \in \mathcal{H}_{a,m}(\mathcal{X}, \mathcal{Y}) : P_-(xy) \geq r\}$$

where  $\mathcal{X} = \{1, \dots, X\}$  and  $\mathcal{Y} = \{1, \dots, Y\}$  and  $1 \leq X, Y \leq m$  are arbitrary integers with  $R$  and  $r$  in reasonably large ranges.

We remark that using elementary sieving arguments one can extend the result of Theorem 13 to counting  $(x, y) \in \mathcal{H}_{a,m}$  such that  $x$  is of the largest possible multiplicative order modulo  $m$  (and thus so is  $y$ ) which is given by the *Carmichael function*  $\lambda(n)$ . In particular, when  $m = p$  is a prime, this addresses the problem of distribution of the points  $(x, y) \in \mathcal{H}_{a,m}$  where  $x$  is a primitive root modulo  $p$ , for example, see [17, 123]. Proofs of these results usually follow the same standard lines as the proof of Theorem 13, except that instead of (1) one uses the bound of the same strength on Kloosterman sums (2) twisted with multiplicative characters

$$\sum_{\substack{(x,y) \in \mathcal{H}_m \\ 1 \leq x,y \leq m}} \chi(x) \mathbf{e}_m(rx + sy) \ll (m \gcd(r, s, m))^{1/2+o(1)}.$$

There are still some delicate issues of getting the  $m^{o(1)}$  term as small as possible. A certain modification of this question has been studied in [230].

We also note that several very interesting results have recently been obtained in [149] about points  $(x, y) \in \overline{\mathcal{H}}_{a,m}$  such that  $x$  and  $y$  have restricted  $g$ -ary expansions to some fixed base  $g \geq 2$ , see also [151].

Finally, we note that the dual question about the arithmetic structure of the ratio  $(xy - a)/m$  for  $(x, y) \in \mathcal{H}_{a,m}$  is also of interest and may have various applications. For example, in [186] such ratios without small prime divisors have been studied, which in turn has been important for yet another number theoretic question.

## 4 Geometric Properties of $\mathcal{H}_{a,m}$

### 4.1 Distances

We observe that the asymptotic formulas (12) and (13) have a natural interpretation as the bounds on the power moments and the distribution function

of the distances between an element  $x \in \{1, \dots, m\}$  with  $\gcd(x, m) = 1$  and its modular inverse. Several results about the average (over  $a$ ) value of power moments of distances can be found in [133, 134, 135, 136, 137, 138], see also references therein.

We now define the *width*  $w_{a,m}$  of the set  $\overline{\mathcal{H}}_{a,m}$ :

$$w_{a,m} = \max \{|x - y| : (x, y) \in \overline{\mathcal{H}}_{a,m}\}.$$

We also put

$$w_m = w_{1,m}$$

for the width of  $\overline{\mathcal{H}}_m$ , which has been the main object of study of [75, 121, 123].

Using Theorem 13 one easily derives that

$$w_{a,m} = m + O(m^{3/4+o(1)}). \quad (23)$$

Using the same arguments as in [123], one can obtain a more precise expression for the factor  $m^{o(1)}$ .

On the other hand, it has been noticed in [121] that

$$m - w_m \geq \lceil 2\sqrt{m-1} \rceil$$

with equality for all  $m$  of the form

$$m = k^2 + \ell k + 1 \quad (24)$$

with integers  $k$  and  $\ell$  such that  $k > 0$ ,  $0 \leq \ell < 2\sqrt{k} + 1$  and hence

$$\liminf_{m \rightarrow \infty} \frac{m - w_m}{\sqrt{m}} = 2. \quad (25)$$

**Question 19.** *Show that there are infinitely many primes  $m = p$  of the form (24) with  $0 \leq \ell < 2\sqrt{k} + 1$ .*

As a curiosity, we recall the following, it has been noted in [75], that  $m - w_m \leq \sqrt{8m}$  for all positive integers  $m = 2^s$  with  $s \in \mathbb{Z}$ . Indeed, if  $s$  is even, then  $m = (2^{s/2} - 1)^2 + 2(2^{s/2} - 1) + 1$  is of the form (24). If  $s$  is odd, then this follows from

$$(2^{(s+1)/2} - 1)(2^s - 2^{(s+1)/2} - 1) \equiv 1 \pmod{2^s}.$$

In the opposite direction it is shown in [75] that

$$\limsup_{m \rightarrow \infty} \frac{m - w_m}{\sqrt{m}} = \infty. \quad (26)$$

Furthermore, analogues of (25) and (26) also hold for prime values  $m = p$ :

$$\liminf_{p \rightarrow \infty} \frac{p - w_p}{\sqrt{p}} = 2 \quad \text{and} \quad \limsup_{p \rightarrow \infty} \frac{p - w_p}{\sqrt{p}} = \infty,$$

which follow from the following two results given in [75].

**Theorem 20.** *For infinitely many primes  $p$ , we have*

$$p - w_p \leq 2\sqrt{p} + \frac{\sqrt{p}}{\log p}.$$

*Proof.* Let  $\varepsilon = 1/(4 \log Q)$ . Using [29] one can show that for sufficiently large  $Q$ , there is a prime  $p$  in the interval  $((1 - \varepsilon)Q, Q]$  such that  $p - 1$  has a divisor  $d$  in the interval  $((1 - 2\varepsilon)\sqrt{Q}, (1 - \varepsilon)\sqrt{Q}]$ . If we write  $p - 1 = df$ , then  $w_p \geq p - f - d$ . But, if  $Q$  is so large that  $\varepsilon \leq 0.01$ , then

$$f + d = \frac{p - 1}{d} + d \leq \frac{x}{(1 - 2\varepsilon)\sqrt{Q}} + (1 - \varepsilon)\sqrt{Q} \leq (2 + 3\varepsilon)\sqrt{p},$$

which implies the desired result.  $\square$

**Theorem 21.** *Let  $f(M)$  be any positive function tending monotonically to zero as  $M \rightarrow \infty$ . Then the inequality*

$$m - w_m \geq m^{1/2}(\log m)^{\kappa/2}(\log \log m)^{3/4}f(m)$$

*holds:*

- *for all positive integers  $m \leq M$ , except for possibly  $o(M)$  of them,*
- *for all primes  $m = p \leq M$  except for possibly  $o(M/\log M)$  of them.*

*Proof.* Let  $M$  be large and set

$$z = (\log M)^{\kappa/2}(\log \log M)^{3/4}f(M/2).$$

It suffices to show  $m - w_m \leq zm^{1/2}$  for  $o(M)$  of integers  $m$  between  $M/2$  and  $M$ . Without loss of generality, suppose  $f(M) \geq 1/\log \log M$  for all  $M > 10$ .

We define  $\mathcal{J}_k$  to be the set of positive integers  $m \in (M/2, M]$  for which  $m - w_m \leq ym^{1/2}$  and such that there are  $(x, y) \in \overline{\mathcal{H}}_m$  with  $w_m = y - x$  and  $x(m - y) = km - 1$ .

By the arithmetic-geometric mean inequality, for every  $m \in \mathcal{J}_k$ , we have

$$\frac{m - w_m}{2} = \frac{m - y + x}{2} \geq \sqrt{x(m - y)} = \sqrt{km - 1}. \quad (27)$$

Thus  $\mathcal{J}_k = \emptyset$  for  $k \geq z^2 + 1$ . Suppose  $1 \leq k < z^2 + 1$ ,  $m \in \mathcal{J}_k$ ,  $(x, y) \in \overline{\mathcal{H}}_m$  and  $x(m - y) = km - 1$ . Then

$$\sqrt{km/2 - 1} \leq \max(x, m - y) \leq z\sqrt{M}.$$

By Lemma 8,

$$\#\mathcal{J}_k \leq H(M, \sqrt{km/2 - 1}, z\sqrt{M}; \mathcal{T}_k) \ll \frac{kM(\log(3z^2/k))^\kappa}{\varphi(k)(\log M)^\kappa(\log \log M)^{3/2}}$$

which after simple calculations leads to the estimate

$$\sum_{1 \leq k < z^2 + 1} \#\mathcal{J}_k = o(M)$$

and proves the first part of the theorem.

The proof of the second part is completely analogous.  $\square$

The following questions have been formulated as conjectures in [75], where one can also find some heuristic arguments in their support.

**Question 22.** *Let  $g(M)$  be any positive function tending monotonically to  $\infty$  as  $M \rightarrow \infty$ . Show that the inequality*

$$m - w_m \leq m^{1/2}(\log m)^{\kappa/2}(\log \log m)^{3/4}g(m)$$

*holds:*

- *for all positive integers  $m \leq M$ , except for possibly  $o(M)$  of them,*
- *for all primes  $m = p \leq M$  except for possibly  $o(M/\log M)$  of them.*

**Question 23.** *Prove that  $m - w_m \leq m^{1/2}(\log m)^{\kappa/2+1/2+o(1)}$  for  $m \rightarrow \infty$ .*

Even a weaker form of Question 23 with just  $m^{1/2+o(1)}$  is already of great interest and would have some interesting applications, see [124].

Besides the extreme and average values of the distances between an element and its modular inverse it is also interesting to study the number of distinct differences between  $x$  and  $y$  for  $(x, y) \in \overline{\mathcal{H}}_{a,m}$ .

**Question 24.** *Estimate the cardinality of the sets*

$$\begin{aligned}\mathcal{D}_{a,m} &= \{|x - y| : (x, y) \in \overline{\mathcal{H}}_{a,m}\}, \\ \mathcal{D}_{a,m}^\pm &= \{x - y : (x, y) \in \overline{\mathcal{H}}_{a,m}\}, \\ \mathcal{S}_{a,m} &= \{x + y : (x, y) \in \overline{\mathcal{H}}_{a,m}\}.\end{aligned}$$

It is easy to see that the sets  $\mathcal{D}_{a,m}$  and  $\mathcal{D}_{a,m}^\pm$  are closely related to each other due to symmetry of points on  $\overline{\mathcal{H}}_{a,m}$ .

Clearly the part of Question 24 concerning  $\mathcal{D}_{a,m}$  is equivalent to counting  $u = 0, \dots, m-1$  for which the quadratic congruence

$$x(x + u) \equiv a \pmod{m}$$

has a solution  $x$  with  $1 \leq x < m - u$ . In the case of  $\mathcal{S}_{a,m}$  one needs to count  $u = 0, \dots, \pm 2(m-1)$  for which

$$x(u - x) \equiv a \pmod{m}$$

has a solution  $x$  with  $1 \leq x < u$ ,

For prime  $m = p$  this question has been studied in [182] where an explicit formula

$$\#\mathcal{D}_{a,p} = \frac{1}{4} \left( p + 1 + \left( \frac{a}{p} \right) (1 + (-1)^{(p-1)/2}) \right).$$

is given, where  $(a/p)$  denotes the *Legendre symbol* of  $a$  modulo  $p$ . It has been shown in [70] that the argument of [182] can also be used to derive explicit formulas for  $\mathcal{D}_{a,p}^\pm$  and  $\mathcal{S}_{a,p}$ . However in the case of composite  $m$  studying these quantities is more complicated and sometimes leads to some surprising discoveries. In particular, it is shown in [70, Theorem 16] that for  $a = 1$  we have

$$\liminf_{m \rightarrow \infty} \frac{\#\mathcal{D}_{1,m}^\pm \log \log m}{\#\mathcal{S}_{1,m}} < \infty \quad \text{and} \quad \limsup_{m \rightarrow \infty} \frac{\mathcal{D}_{1,m}^\pm}{\#\mathcal{S}_{1,m} \log \log m} > 0, \quad (28)$$

see also [122]. These results also have some interesting combinatorial interpretation.

In [182] an analogue of Question 24 concerning  $\mathcal{D}_{a,p}^\pm$  is also studied when  $x$  and  $y$  range over prescribed intervals, however the method of [182] does not immediately apply to the case of composite moduli  $m$ .

A similar question can also be asked about Euclidean distances between distinct points of  $\overline{\mathcal{H}}_{a,m}$  and also between the origin and points of  $\overline{\mathcal{H}}_{a,m}$ .

**Question 25.** *Estimate the cardinality of the sets*

$$\mathcal{E}_{a,m} = \{ \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2} : (x_1, y_1), (x_2, y_2) \in \overline{\mathcal{H}}_{a,m} \}$$

and

$$\mathcal{F}_{a,m} = \{ \sqrt{x^2 + y^2} : (x, y) \in \overline{\mathcal{H}}_{a,m} \}.$$

The author is grateful to Arne Winterhof for the observation that if  $m = p$  is a prime then  $\#\mathcal{F}_{a,p}$  can be evaluated explicitly. Indeed if  $u \equiv x^2 + y^2 \pmod{p}$  for  $(x, y) \in \overline{\mathcal{H}}_{a,p}$  then the congruence  $Z^4 - uZ^2 + a^2 \equiv 0 \pmod{p}$  has exactly four roots  $x, p - x, y, p - y$  (in particular, we have two double roots if  $x = y$ ). Since  $(p - x)^2 + (p - y)^2 \neq x^2 + y^2$  we have

$$\#\mathcal{F}_{a,p} = \frac{1}{2} \left( p + \left( \frac{a}{p} \right) \right).$$

Clearly, Theorem 13 can be used to obtain some lower bounds on  $\#\mathcal{D}_{a,m}$  and  $\#\mathcal{E}_{a,m}$ . For example, an easy modification of an argument which leads to the bound (23) yields

$$\#\mathcal{D}_{a,m} \geq m^{1/4+o(1)}.$$

However we are mostly interested in more precise results which should certainly be based on some additional ideas.

We also ask a question of a different flavour, which is about the number of possible directions on the Euclidean plane defined by the pairs of distinct points  $(x_1, y_1), (x_2, y_2) \in \overline{\mathcal{H}}_{a,m}$ .

**Question 26.** *Estimate the cardinality of the set*

$$\mathcal{L}_{a,m} = \left\{ \frac{x_1 - x_2}{y_1 - y_2} : (x_1, y_1), (x_2, y_2) \in \overline{\mathcal{H}}_{a,m}, (x_1, y_1) \neq (x_2, y_2) \right\}.$$

Obviously Questions 25 and 26 are influenced by the *Erdős* and *Kakeya* problems, respectively, see [39, Sections 5.3 and 7.1] and also surveys [32, 120] (we also note the recent remarkable achievement [69, 105]). They can also be asked for points of  $\mathcal{H}_{a,m}(\mathcal{X}, \mathcal{Y})$  for various sets  $\mathcal{X}$  and  $\mathcal{Y}$ .

We note that in the definitions of the sets  $\mathcal{E}_{a,m}$ ,  $\mathcal{F}_{a,m}$  and  $\mathcal{L}_{a,m}$  all distances and angles are computed over the rationals. The same questions can also be asked with similar quantities where calculations are performed modulo  $m$ . Some interesting results in this direction can be found in [70, 107, 122].

Finally, motivated by [21, 22] and some other works one can also ask various questions about the distribution of the angles of elevation  $\arctan(y/x)$  of points  $(x, y) \in \mathcal{H}_{a,m}(\mathcal{X}, \mathcal{Y})$  over the horizontal line.

## 4.2 Convex Hull

We consider the convex closure  $\mathcal{C}_m$  of the point set  $\overline{\mathcal{H}}_m$ . It is not hard to see that  $\mathcal{C}_m$  is always a convex polygon with nonempty interior, except when  $m = 2, 3, 4, 6, 8, 12, 24$ , see [124].

Following [124], we denote by  $v(m)$  the number of vertices of  $\mathcal{C}_m$  and by  $V(M)$  its average value,

$$V(M) = \frac{1}{M-1} \sum_{m=2}^M v(m).$$

First of all we notice that by a result of [7] a convex polygon of area  $S$  may have at most  $O(S^{1/3})$  integer vertices, thus we immediately conclude that  $v(m) \ll m^{2/3}$ . It is shown in [74] that a combination of the bound of [7] with Theorem 13 leads to a stronger estimate:

$$v(m) \leq m^{7/12+o(1)}. \quad (29)$$

Indeed, one can see from Theorem 13 that all vertices of  $\mathcal{C}_m$  belong to one of the rectangles with one side length  $m$  and the other side length  $m^{3/4+o(1)}$  which are adjacent to one of the sides of the square  $[0, m-1] \times [0, m-1]$ . Now considering the intersections of  $\mathcal{C}_m$  with each of these rectangles (which remains convex) and applying the result of [7], we obtain (29). The bound (29) has recently been improved in [125] as

$$v(m) \leq m^{1/2+o(1)} \quad (30)$$

for any integer  $m \geq 1$  and as

$$v(m) \leq m^{5/12+o(1)} \quad (31)$$

for  $m$  which are almost squarefree (in particular, for almost all  $m$ ). The proof of (31) is based on some geometric arguments, and thus on Lemmas 11 and 12, and the bound on the number of solutions to bivariate quadratic Diophantine equations in a box given by Lemma 10. Furthermore, the same bounds hold for the convex hulls of arbitrary hyperbolas  $\overline{\mathcal{H}}_{a,m}$ .

More interestingly, one can obtain another bound, which is much better in some cases and relies on more specific properties of  $\overline{\mathcal{H}}_m$

$$v(m) \leq T(m-1)m^{o(1)}, \quad (32)$$

see [124], where  $T(k)$  is defined in Section 2.4.

The lower bound

$$v(m) \geq 2(\tau(m-1) - 1) \quad (33)$$

is also given in [124]. Furthermore, it is shown in [124] that in fact  $v(m) = 2(\tau(m-1) - 1)$  whenever  $T(m-1) \leq 5$ . Thus, this and the bound (32) explain why Lemma 9 comes into play. On the other hand, it is shown in [74] that  $v(m) > 2(\tau(m-1) - 1)$  for a set of  $m$  of positive asymptotic density. On the other hand, improving the previous estimate of [75], it is shown in [74] that [2, Theorem 2.1] can be used to derive that

$$v(p+1) \geq \exp\left(\left(\frac{5 \log 2}{12} + o(1)\right) \frac{\log p}{\log \log p}\right).$$

for infinitely many primes  $p$ . In particular this shows, in a strong form, that sometimes  $v(m)$  and  $\tau(m-1)$  are vastly different orders of magnitude.

One can also find in [124] several efficient algorithms for computing  $v(m)$ , together with their complexity analysis.

Numerical calculations show that while the behaviour of  $v(m)$  is not adequately described by any of the above bounds, the lower bound (33) seems to be more precise than (29) and (32).

It is quite natural to view the points of  $\overline{\mathcal{H}}_m$  as being randomly distributed in the square  $[0, m] \times [0, m]$  (which is supported by the theoretic results which we have presented in Sections 3.1 and 3.2) and then appeal to the following result of [156, Satz 1]. Let  $\mathcal{R}$  be a convex polygon in the plane with  $r$  vertices and let  $P_i$ ,  $i = 1, \dots, n$ , be  $n$  points chosen at random in  $\mathcal{R}$  with uniform



distribution. Let  $X_n$  be the number of vertices of the convex closure of the points  $P_i$ , and let  $E(X_n)$  be the expectation of  $X_n$ . Then

$$E(X_n) = \frac{2}{3}r(\log n + \gamma) + c_{\mathcal{R}} + o(1), \quad (34)$$

where  $\gamma = 0.577215\dots$  is the Euler constant, and  $c_{\mathcal{R}}$  depends on  $\mathcal{R}$  and is maximal when  $\mathcal{R}$  is a regular  $r$ -gon or is affine equivalent to a regular  $r$ -gon. In particular, for the unit square  $\mathcal{R} = [0, 1]^2$  we have

$$c_{\mathcal{R}} = -\frac{8}{3}\log 2.$$

Using (34) with  $r = 4$ , it seems plausible to conjecture that for most  $m$

$$v(m) \approx h(m),$$

where

$$h(m) = \frac{8}{3}(\log \varphi(m) + \gamma - \log 2).$$

However, surprisingly enough, the numerical results of [124] show that  $V(M)$  deviates from

$$H(M) = \frac{1}{M-1} \sum_{m=2}^M h(m) = \frac{8}{3}(\log M + \gamma + \eta - 1 - \log 2 + o(1)),$$

where

$$\eta = \sum_{p \text{ prime}} \frac{\log(1 - 1/p)}{p} = -0.580058\dots,$$

quite significantly, and is apparently larger than  $H(M)$  by a fixed factor. Some partial explanation to this phenomenon has been given in [124] and suggests that for each  $m$ , the convex hull  $\mathcal{C}_m$ , besides some “random” points, also contains a “regular” component with  $2(\tau(m-1) - 1)$  points associated with divisors of  $m-1$  whose average contribution

$$\frac{1}{M-1} \sum_{m=2}^M 2(\tau(m-1) - 1) \sim 2 \log M$$

is of the same order of magnitude as the size of  $H(M)$ .

It is also shown [124] that this affect is specific to the points of  $\overline{\mathcal{H}}_m$  and disappears for the convex hull of points on a “generic” curve which behaves in much better agreement with (34) than  $v(m)$ .

Clearly since  $(1, 1), (m-1, m-1) \in \overline{\mathcal{H}}_m$  the diameter of  $\overline{\mathcal{H}}_m$  takes the largest possible value  $\sqrt{2}(m-2)$ . However for the other values of  $a$  the question about the diameter of  $\overline{\mathcal{H}}_{a,m}$  is more interesting.

**Question 27.** *Estimate the diameter*

$$\Delta_{a,m} = \max\{\sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2} : (x_1, y_1), (x_2, y_2) \in \overline{\mathcal{H}}_{a,m}\}.$$

### 4.3 Visible Points

For two sets of integers  $\mathcal{X}$  and  $\mathcal{Y}$  we denote

$$\mathcal{G}_{a,m}(\mathcal{X}, \mathcal{Y}) = \#\{(x, y) \in \mathcal{H}_{a,m}(\mathcal{X}, \mathcal{Y}) : \gcd(x, y) = 1\}$$

and also, following our usual agreement, we put  $\mathcal{G}_m(\mathcal{X}, \mathcal{Y}) = \mathcal{G}_{1,m}(\mathcal{X}, \mathcal{Y})$ .

Clearly  $\mathcal{G}_{a,m}(\mathcal{X}, \mathcal{Y})$  is the set of points  $(x, y) \in \mathcal{H}_{a,m}(\mathcal{X}, \mathcal{Y})$  which are “visible” from the origin (that is, which are not “blocked” by other points with integer coordinates).

The following estimate is obtained in [168] for  $\mathcal{G}_m(\mathcal{X}, \mathcal{Y})$  but its extension to the general case is immediate and we present it here (in fact we also simplify the argument).

**Theorem 28.** *Let  $\mathcal{X} = \{1, \dots, X\}$  and  $\mathcal{Y} = \{1, \dots, Y\}$  where  $1 \leq X, Y \leq m$  are arbitrary integers. For all integers  $m$  with  $XY \geq m^{3/2}$  we have*

$$\#\mathcal{G}_{a,m}(\mathcal{X}, \mathcal{Y}) = \frac{6}{\pi^2} \cdot \frac{XY}{m} \prod_{p|m} \left(1 + \frac{1}{p}\right)^{-1} + O\left(X^{1/2}Y^{1/2}m^{-1/4+o(1)}\right),$$

where the product is taken over all prime numbers  $p \mid m$ .

*Proof.* For an integer  $z$  we let

$$\mathcal{H}_{a,m}(z; \mathcal{X}, \mathcal{Y}) = \{(x, y) \in \mathcal{H}_{a,m}(\mathcal{X}, \mathcal{Y}) : z \mid \gcd(x, y)\}.$$

By the inclusion-exclusion principle, we write

$$\#\mathcal{G}_{a,m}(\mathcal{X}, \mathcal{Y}) = \sum_{z=1}^{\infty} \mu(z) \#\mathcal{H}_{a,m}(z; \mathcal{X}, \mathcal{Y}).$$

Clearly

$$\mathcal{H}_{a,m}(z; \mathcal{X}, \mathcal{Y}) = \emptyset$$

if  $\gcd(z, m) > 1$  or  $z > m$ . For  $\gcd(z, m) = 1$ , writing

$$x = zs \quad \text{and} \quad y = zt, \tag{35}$$

we have

$$\mathcal{H}_{a,m}(z; \mathcal{X}, \mathcal{Y}) = \{(zs, zt) : st \equiv az^{-2} \pmod{m}, \\ 1 \leq s \leq X/z, 1 \leq t \leq Y/z\}.$$

Now, we define

$$R = \lceil X^{1/2}Y^{1/2}m^{-3/4} \rceil \quad \text{and} \quad Q = \lceil X^{1/2}Y^{1/2}m^{-1/2} \rceil,$$

and note that

$$XY/Q^2 \leq m.$$

A variant of Theorem 13 gives

$$\#\mathcal{H}_{a,m}(z; \mathcal{X}, \mathcal{Y}) = \frac{XY\varphi(m)}{z^2m^2} + O(m^{1/2+o(1)}),$$

which we apply for “small”  $z \leq R$ .

We also note that for each  $z$ , the product  $r = st \leq XY/z^2$ , where  $s$  and  $t$  are given by (35), belongs to a fixed residue class modulo  $m$  and thus can take at most  $XY/z^2m + 1$  possible values. For each fixed  $r \leq XY/z^2 \leq XY \leq m^2$ , there are  $\tau(r) = r^{o(1)} = m^{o(1)}$  pairs  $(s, t)$  of integers  $s$  and  $t$  with  $r = st$ , see (8). Therefore,

$$\#\mathcal{H}_{a,m}(z; \mathcal{X}, \mathcal{Y}) \leq \left( \frac{XY}{z^2m} + 1 \right) m^{o(1)},$$

which we apply for “medium”  $z$  with  $Q \geq z > R$ .

We observe that Lemma 1 yields the bound

$$\sum_{\substack{z=1 \\ \gcd(z,m)=1}}^m \mathbf{e}_m(Az^{-2} + Bz) \ll \gcd(A, B, m)^{1/2} m^{1/2+o(1)}.$$

Using the same arguments as in the proof of Theorem 13, we deduce that for the number of positive integers  $z \leq Z$  with  $az^{-2} \equiv w \pmod{m}$  with some  $w \leq W$  is  $ZW/m + O(m^{1/2+o(1)})$ .

We now remark that  $az^{-2} \equiv r \pmod{m}$  where, as before,

$$r = st \leq XY/z^2 \leq XY/Q^2 \leq m.$$

Furthermore, for every  $z$  the value of  $r$  is uniquely defined and leads to at most  $\tau(r) = m^{o(1)}$  possible pairs  $(s, t)$ . Hence, the total contribution from “large”  $z \geq Q$  can be estimated as

$$\begin{aligned} \sum_{m \geq z \geq Q} \#\mathcal{H}_{a,m}(z; \mathcal{X}, \mathcal{Y}) &\leq \sum_{\nu=0}^{\lceil 2 \log m \rceil} \sum_{2^{\nu+1}Q > z \geq 2^\nu Q} \#\mathcal{H}_{a,m}(z; \mathcal{X}, \mathcal{Y}) \\ &\leq \sum_{\nu=0}^{\lceil 2 \log m \rceil} \left( 2^{\nu+1}Q \cdot \frac{XY}{m(2^\nu Q)^2} + m^{1/2} \right) m^{o(1)} \\ &\leq \sum_{\nu=0}^{\lceil 2 \log m \rceil} \left( \frac{XY}{2^\nu m Q} + m^{1/2} \right) m^{o(1)} \\ &= \frac{XY}{Q} m^{-1+o(1)} + m^{1/2+o(1)}. \end{aligned}$$

Combining the above bounds and recalling our choice of  $R$  and  $Q$  (which optimises the error term), we derive the desired result.  $\square$

In particular, under the conditions of Theorem 28

$$\#\mathcal{G}_{a,m}(\mathcal{X}, \mathcal{Y}) \sim \frac{6}{\pi^2} \cdot \frac{XY}{m} \prod_{p|m} \left( 1 + \frac{1}{p} \right)^{-1}$$

provided that  $XY \geq m^{3/2+\varepsilon}$  for some fixed  $\varepsilon > 0$ .

It is noticed in [46] that Theorem 28 maybe of use for some Diophantine approximation questions, see Section 5.17.

A multidimensional version of Theorem 28 has been derived in [183]. For the dimension  $s = 3$  it is based on Theorem 16. For  $s \geq 4$  the proof is based on various bounds for multiplicative character sums in the same style as in [169, 176].

Visible points satisfying general polynomial congruences have been studied in [181]. However in [181] nontrivial results have been obtained only “on average” (either over some families of congruences or over some moduli). Recently, a nontrivial result for “individual” congruences has been given in [52].

Using the technique of [52], together with Theorem 30 below, one can probably tackle the following problem:

**Question 29.** *Extend Theorem 28 to intervals of the form*

$$\mathcal{X} = \{U + 1, \dots, U + X\} \quad \text{and} \quad \mathcal{Y} = \{V + 1, \dots, V + Y\}$$

*with arbitrary  $U$  and  $V$ .*

We also refer to [145] for further generalisations.

## 4.4 Concentration of Points

For a positive integer  $Z < p$  and arbitrary integers  $U$  and  $V$ , we denote by  $T_{a,p}(Z; U, V)$  the number of points  $(x, y) \in \mathcal{H}_{a,p}$  which belong to the square  $[U + 1, U + Z] \times [V + 1, V + Z]$ .

We remark that Theorem 13 implies that  $T_{a,p}(Z; U, V) = (1 + o(1))Z^2/p$  if  $Z \geq p^{3/4+\varepsilon}$  for a fixed  $\varepsilon > 0$ , and also gives a nontrivial upper bound  $T_{a,p}(Z; U, V) = o(Z)$  if  $Z \geq p^{1/2+\varepsilon}$  and  $Z = o(p)$  as  $p \rightarrow \infty$ . These results seem to be the limit of what can be achieved within the standard exponential sum techniques and currently available estimates on incomplete Kloosterman sums.

However, in [51] improving the previous result of [50], the following estimate has been given:

**Theorem 30.** *There exists some absolute constant  $\eta > 0$  such that for any positive integer  $Z < p$ , uniformly over arbitrary integers  $U$  and  $V$ , we have*

$$T_{a,p}(Z; U, V) \leq \begin{cases} Z^{4/3+o(1)}p^{-1/3} + Z^{o(1)} & \text{for any } U \text{ and } V, \\ Z^{3/2+o(1)}p^{-1/2} + Z^{o(1)} & \text{if } U = V. \end{cases}$$

Several more related estimates are given in [12, 36, 37, 60, 61, 96].

## 4.5 Arithmetic Functions on Points on $\mathcal{H}_{a,m}$

A modification of the proof of Theorem 28 has lead to the asymptotic formula (19). There is little doubt that it can also be extended to the case where variables are taken intervals of different lengths and also to the sums

$$\sum_{(x,y) \in \mathcal{H}_m(\mathcal{X}, \mathcal{Y})} |\mu(xy)|$$

under the same conditions on the sets  $\mathcal{X}$  and  $\mathcal{Y}$  as in Theorem 28.

For a prime  $p$ , asymptotic formulas for the average values

$$\sum_{\substack{(x,y) \in \mathcal{H}_{a,p}(X,Y) \\ x \neq y}} \frac{\varphi(|x-y|)}{|x-y|} \quad \text{and} \quad \sum_{\substack{(x,y) \in \mathcal{H}_{a,p}(X,X) \\ x \neq y}} \varphi(|x-y|)$$

are given in [172].

It is also interesting to study sums of other arithmetic functions on  $(x, y) \in \mathcal{H}_m(\mathcal{X}, \mathcal{Y})$ .

**Question 31.** *For intervals*

$$\mathcal{X} = \{U + 1, \dots, U + X\} \quad \text{and} \quad \mathcal{Y} = \{V + 1, \dots, V + Y\}$$

of length  $X, Y \leq m$ ,

- *obtain nontrivial bounds for the sums*

$$\sum_{(x,y) \in \mathcal{H}_{a,m}(\mathcal{X}, \mathcal{Y})} \mu(xy) \quad \text{and} \quad \sum_{(x,y) \in \mathcal{H}_{a,m}(\mathcal{X}, \mathcal{Y})} \left( \frac{x}{y} \right),$$

where  $(x/y)$  is the Jacobi symbol of  $x$  modulo  $y$ , which we also extend to even values of  $y$  by simply putting  $(x/y) = 0$  in this case;

- *obtain estimates or asymptotic formulas for the sums*

$$\sum_{(x,y) \in \mathcal{H}_{a,m}(\mathcal{X}, \mathcal{Y})} \tau(|x-y|) \quad \text{and} \quad \sum_{(x,y) \in \mathcal{H}_{a,m}(\mathcal{X}, \mathcal{Y})} \omega(|x-y|).$$

We remark that in the case when  $\mathcal{X}$  and  $\mathcal{Y}$  are very large (compared to  $m$ ) intervals of the form

$$\mathcal{X} = \{X + 1, \dots, 2X\} \quad \text{and} \quad \mathcal{Y} = \{Y + 1, \dots, 2Y\} \quad (36)$$

the bound on the sum of Jacobi symbol  $(x/y)$  has been given in [213]. In fact, the bound of [213] applies to even more general bilinear sums and asserts that for any  $\varepsilon > 0$

$$\sum_{\substack{(x,y) \in \mathcal{H}_{a,m}(\mathcal{X}, \mathcal{Y}) \\ xy \leq Z}} \alpha_x \beta_y \left( \frac{x}{y} \right) \ll XY^{15/16+\varepsilon} + X^{15/16+\varepsilon} Y \quad (37)$$

provided that

$$m \leq (\min\{X, Y\})^{\varepsilon/3}, \quad (38)$$

where  $\mathcal{X}$  and  $\mathcal{Y}$  are of the form (36),  $Z$  is an arbitrary parameter and the sequences  $\alpha_x$  and  $\beta_y$  are supported on  $\mathcal{X}$  and  $\mathcal{Y}$ , respectively, and satisfy

$$|\alpha_x| \leq 1, \quad x \in \mathcal{X} \quad \text{and} \quad |\beta_y| \leq 1, \quad y \in \mathcal{Y}.$$

Since the sum on the left hand side of (37) does not exceed  $XY/m + \min\{X, Y\}$  we see that the bound is nontrivial only if

$$m \leq (\min\{X, Y\})^{1/16-\varepsilon}. \quad (39)$$

Comparing (38) and (39) we see that (37) may only be nontrivial if

$$\min\{X, Y\} \geq m^{64}.$$

Some modifications of the argument of [213] may reduce the exponent 64, but certainly not below 16, while in Question 31 we ask about much shorter sums.

## 5 Applications

### 5.1 The Lehmer Problem

One of the most natural and immediate applications of the uniformity of distribution results outlined in Section 3.1 is a positive solution to the *Lehmer problem*, see [104, Problem F12], about the joint distribution of the parity of  $x$  and  $y$  for  $(x, y) \in \mathcal{H}_{a,m}(\mathcal{X}, \mathcal{Y})$  with some intervals

$$\mathcal{X} = \{U + 1, \dots, U + X\} \quad \text{and} \quad \mathcal{Y} = \{V + 1, \dots, V + Y\}.$$

This distribution is naturally expected to be close to uniform (that is, each parity combination is taken about in 25% of the cases) for any odd  $m \geq 1$  and sufficiently large  $X$  and  $Y$ . The Lehmer problem can easily be reformulated as a question about the cardinality of  $\#\mathcal{H}_{a,m}(\tilde{\mathcal{X}}, \tilde{\mathcal{Y}})$  for some  $a$  and some other sets  $\tilde{\mathcal{X}}$  and  $\tilde{\mathcal{Y}}$  of about  $X/2$  and  $Y/2$  consecutive integers, respectively. Indeed, we are interested in solutions to the congruence

$$(2\tilde{x} + \vartheta_1)(2\tilde{y} + \vartheta_2) \equiv a \pmod{m}$$

with some fixed  $\vartheta_1, \vartheta_2 \in \{0, 1\}$  and

$$\frac{U+1-\vartheta_1}{2} \leq \tilde{x} \leq \frac{U+X-\vartheta_1}{2}, \quad \frac{V+1-\vartheta_2}{2} \leq \tilde{y} \leq \frac{V+Y-\vartheta_2}{2}.$$

It remains to notice that the above congruence is equivalent to

$$(\tilde{x} + 2^{-1}\vartheta_1)(\tilde{y} + 2^{-1}\vartheta_2) \equiv 4^{-1}a \pmod{m}$$

(where the inversion is taken modulo  $m$ ), which after a shift of variables takes the desired shape.

Close links between the Lehmer problem and bounds of Kloosterman sums (2) has been first observed in [218, 219]. The question and the above approach have been extended in several directions, see [5, 56, 57, 132, 133, 134, 136, 139, 140, 141, 145, 161, 207, 209, 210, 214, 216, 220, 221, 222, 223, 225] and references therein. In particular, in multidimensional generalisations, instead of the bound (1) more general bounds of incomplete or multiple Kloosterman sums

$$\sum_{U_1+1 \leq x_1 \leq U_1+X_1} \dots \sum_{U_n+1 \leq x_n \leq U_n+X_n} \mathbf{e}_m(r_1x_1 + \dots + r_nx_n + s(x_1 \dots x_n)^{-1}),$$

have been frequently used. However, it has turned out that for multivariate analogues of the Lehmer problem, and a number of similar questions, bounds of character sums provide a more efficient tool than Kloosterman sums (2), see [176], where Lemmas 2 and 3 (for prime  $m = p$ ) and the bound (6) have been used to improve several previous results.

Some ternary additive problems with points  $(x, y) \in \mathcal{H}_{a,m}$  satisfying additional divisibility conditions are considered in [142]. The result of [142] has been improved in [184] where it is shown that one in fact can deal with binary additive problems with such numbers.

A generalisation of the original problem to joint distribution of arbitrary monomials and two arbitrary progressions is given in [174], which improves and generalises some results of [212].

Furthermore, a similar problem has also appeared in a very different context related to cryptography. Indeed, it has been shown in [35] that the conjecture of [101] on the cyclical distinctness of so-called  $\ell$ -sequences modulo  $p$  can be reformulated as the conjecture that for any prime  $p$  and pair of integers  $(a, d) \neq (1, 1)$  with

$$\gcd(d, p-1) = 1, \quad 0 < |a| < p/2, \quad |d| < p/2,$$



except for six explicitly listed triples of  $(p, a, d)$ , at least one residue modulo  $p$  of  $ax^d$  is odd when  $x$  runs through all even residues modulo  $p$ , that is, that  $ax^d \equiv y \pmod{p}$  for some

$$x \in \{2, 4, \dots, p-1\} \quad \text{and} \quad y \in \{1, 3, \dots, p-2\}.$$

In [102] this conjecture has been established for a wide class of triples  $(p, d, a)$  and also for all such triples. Finally, in [35] it has been proved for all triples  $(p, d, a)$  provided that  $p$  is large enough. Clearly  $d = -1$  is related to the Lehmer conjecture. Recently, a decisive progress in a generalised Lehmer conjecture has been made in [34]. It is certainly interesting to see how much the methods of [34, 35] can be expanded and carried over to other problems. For examples, in the most general form one can ask about the existence and distribution of solutions to the congruence

$$x_1^{d_1} \dots x_s^{d_s} \equiv a \pmod{p}, \quad 1 \leq x_1, \dots, x_s < p$$

in  $s$  arithmetic progressions  $x_i \equiv b_i \pmod{k_i}$ ,  $i = 1, \dots, s$ .

## 5.2 Distribution of Angles in Some Point Sets

A version of Theorem 13 has been used in [22] to study the distribution of angles between visible points (viewed from the origin) in a dilation of a certain plain region  $\Omega \subseteq [0, 1]^2$ . More precisely, for  $\Omega \subseteq [0, 1]^2$  and a sufficiently large  $Q$ , we define

$$\Omega_Q = \{(Q\alpha, Q\beta) : (\alpha, \beta) \in \Omega\}.$$

We now consider  $\#\mathcal{F}_\Omega(Q)$  angles between the horizontal line and the points of the set

$$\mathcal{F}_\Omega(Q) = \{(x, y) \in \Omega_Q \cap \mathbb{Z}^2 : \gcd(x, y) = 1\}.$$

The distribution of these angles is studied in [22] and shown to exhibit a somewhat unexpected behaviour.

A slight generalisation of Theorem 13 has also played an important role in the study of angles defined by some other point sets [21], see also [25, 26, 196].

## 5.3 Distribution of the Trajectory Length in the Periodic Lorentz Gas

Links between Theorem 13 and some problems of mathematical physics can be found in [24, 27, 43, 44]. Namely, assume that a particle moves along a

straight line in a  $d$ -dimensional lattice until it falls in a  $\delta$ -neighbourhood of a lattice point. In [24, 27, 43, 44] the distribution of the trajectory length is studied.

## 5.4 Vertices of Convex Lattice Polygons

Let  $N(r)$  be the number of vertices of the convex hull of the set of the integral lattice points inside of the ball of radius  $R$  centered at the origin, that is, of the set  $\{(x, y) \in \mathbb{Z}^2 : x^2 + y^2 \leq r^2\}$ . It is shown in [13] that for  $1 \leq H \leq R$  we have

$$\frac{1}{H} \int_R^{R+H} N(r) dr = \frac{6 \cdot 2^{2/3}}{\pi} R^{2/3} + O(HR^{-1/3} + H^{-1}R^{2/3} + R^{5/8+o(1)}).$$

A version of Theorem 13 is one of the crucial ingredients of the proof.

## 5.5 Arithmetic Structure of Shifted Products

The main result of [186] on the largest prime divisor of the shifted products  $ab + 1$ , when  $a$  and  $b$  run through some reasonably dense sets of integers of a sufficiently large interval  $[1, N]$ , is based on a variant of Theorem 13. The result of [186] has recently been improved in [147], where it is also shown that the above problem is related to counting  $\#\mathcal{H}_p(\mathcal{X}, \mathcal{Y})$  on average over primes  $p$  for arbitrary sets of integers  $\mathcal{X}, \mathcal{Y} \subseteq \mathbb{Z}$ .

Furthermore, in [130], Theorem 13 and its generalisations given in [169, 176] (that are based on bounds on multiplicative character sums) have been used to study  $k$ th powerfree values of the polynomial  $X_1 \dots X_r - 1$ , see also [81] for some other related results and alternative approaches to problems of this type.

## 5.6 Sums of Divisor Functions over Quadratic Polynomials and Arithmetic Progressions

It has been demonstrated in [41] that results about the distribution of points  $(x, y) \in \mathcal{H}_{a,m}$  in the regions of the form (15) can be used to derive precise asymptotic formulas for sums of the divisors with quadratic polynomials; for example, for the sums

$$S_D(N) = \sum_{n \leq N} \tau(n^2 + D)$$

where  $D \geq 1$  is a squarefree integer.

Furthermore, the strength of estimates on the error terms in asymptotic formulas for sums of some divisor functions over an arithmetic progression

$$S_{a,m}(N) = \sum_{\substack{n \leq N \\ n \equiv a \pmod{m}}} \tau(n)$$

is closely related to the precision of our knowledge of  $\#\mathcal{H}_{a,m}(\mathcal{X}, \mathcal{Y})$ , where  $\mathcal{X}$  and  $\mathcal{Y}$  are sets of consecutive integers and also multidimensional analogues of this question, see [15, 76, 82, 83, 108, 190]. This link becomes transparent if one recalls that a standard approach to evaluating divisor sums is approximating the hyperbolic region  $\{(x, y) : x, y \geq 0, xy \leq N\}$  by a union of “small” rectangles. In fact, as we have mentioned, the proof of Theorem 16 is based on some ideas of [15], where an asymptotic formula is given for the sums  $S_{a,m}(N)$  “on average” over  $a$ . In [190], there are also several results, and conjectures, for similar average values of various restricted versions of the divisor functions  $\tau(n)$ , but with less averaging. These results are also related to the problem of Section 5.7.

## 5.7 Pair Correlation of Fractional Parts of $\alpha n^2$

It is known, see [146, 160], that the spacings between the fractional parts of the sequence  $\alpha n^2$ ,  $n = 1, 2, \dots$ , obey a Poisson distribution for almost all real  $\alpha$ . However no specific example of such  $\alpha$  is known. However [109, Theorem 2] comes very close to giving such an example. Its proof, amongst other technical tools, is also based on tight upper bounds for the divisor function over short arithmetic progressions, which in turn leads to studying points on modular hyperbolas. In particular, we note that [109, Conjecture 2], can be reformulated as the upper bound

$$\#\mathcal{H}_{a,m}(\mathcal{X}, \mathcal{Y}) \ll \frac{\varphi(m)}{m^2} Z^2$$

for the sets  $\mathcal{X} = \mathcal{Y} = \{1, \dots, Z\}$  with an integer  $Z \geq m^{1/2+\varepsilon}$  for any fixed  $\varepsilon$ . Besides, it is shown in [109] that one of the approaches to the distribution of spacings between the fractional parts of  $\alpha n^2$  is via studying the number of solutions of the quadratic congruence

$$x^2 - y^2 \equiv c \pmod{q}, \quad 1 \leq x \leq X, \quad 1 \leq y \leq Y,$$

on average over  $c$  that runs through the reduced residue classes modulo  $q$ . Furthermore, one can find such a bound in [109, Lemma 3]. It is shown in [179] that a slight generalisation of Theorem 16 leads to an improvement of [109, Lemma 3] for some parameter ranges. However, unfortunately in the range relevant to the pair correlation problem the corresponding results of [109] and [179] are essentially of the same strength.

Similar links between the distribution of fractional parts of  $\alpha n^2$ , behaviour of the divisor function in arithmetic progressions and distribution of points on modular hyperbolas have also been exhibited in [190]. It is shown in [178] that Theorem 16 can be used to derive improvements on some of the results of [190].

## 5.8 The Sato–Tate Conjecture in the “Vertical” Aspect

We also recall that Theorem 16 about the distribution of points on  $\mathcal{H}_{a,m}$  on average over  $a$  has been used in studying the so-called “vertical” aspect of the Sato–Tate conjecture for Kloosterman sums (2), see [171]. The relation is provided by the identity  $K_m(r, s) = K_m(1, rs)$  which holds if  $\gcd(r, m) = 1$ . Clearly for the complex conjugated sum we have

$$\overline{K_m(r, s)} = K_m(-r, -s) = K_m(r, s),$$

hence we see that  $K_m(r, s)$  is real. Since by the Weil bound, for any prime  $p$ , we have

$$|K_p(r, s)| \leq 2\sqrt{p}, \quad \gcd(r, s, p) = 1,$$

see [115, Theorem 11.11], we can now define the angles  $\psi_p(r, s)$  by the relations

$$K_p(r, s) = 2\sqrt{p} \cos \psi_p(r, s) \quad \text{and} \quad 0 \leq \psi_p(r, s) \leq \pi.$$

The famous *Sato–Tate* conjecture asserts that, in the “horizontal” aspect, that is, for any fixed non-zero integers  $r$  and  $s$ , the angles  $\psi_p(r, s)$  are distributed according to the *Sato–Tate density*

$$\mu_{ST}(\alpha, \beta) = \frac{2}{\pi} \int_{\alpha}^{\beta} \sin^2 \gamma \, d\gamma,$$

see [115, Section 21.2]. More precisely, if  $\pi_{r,s}(\alpha, \beta; T)$  denotes the number of primes  $p \leq T$  with  $\alpha \leq \psi_p(r, s) \leq \beta$ , the Sato–Tate conjecture predicts that

$$\pi_{r,s}(\alpha, \beta; T) \sim \mu_{ST}(\alpha, \beta) \pi(T), \quad T \rightarrow \infty, \quad (40)$$

for all fixed real  $0 \leq \alpha < \beta \leq \pi$ , where, as usual,  $\pi(T)$  denotes the total number of primes  $p \leq T$ , see [115, Section 21.2]. We remark that for elliptic curves, the Sato–Tate conjecture in its original (and the most difficult) “horizontal” aspect has recently been settled [188], but it still remains open for Kloosterman sums (2). It is shown in [171] that Theorem 16 implies that

$$\frac{1}{4RS} \sum_{0 < |r| \leq R} \sum_{0 < |s| \leq S} \pi_{r,s}(\alpha, \beta; T) \sim \mu_{ST}(\alpha, \beta) \pi(T)$$

provided  $RS \geq T^{1+\varepsilon}$  for some fixed  $\varepsilon > 0$ .

## 5.9 Farey Fractions and Quotients of the Dedekind Eta-function

A result on the average values of some bivariate functions taken over points of  $\mathcal{H}_{a,m}$ , has been obtained in [23] as a tool in the study of the distribution of Farey fractions

$$\mathcal{F}(T) = \{r/s \in \mathbb{Q} : \gcd(r, s) = 1, 1 \leq r < s \leq T\}. \quad (41)$$

The proof of this result is based on some bounds of incomplete Kloosterman sums and is based on the same ideas which have led to Theorem 13.

It has also been used [6] to study the distribution of the quotients of the Dedekind Eta-function  $\eta(z)$ .

## 5.10 Farey Fractions in Residue Classes and the Lang-Trotter Conjecture on Average

The same arguments used in the prove of Theorem 16, can be used to study the distribution of ratios  $x/y$ ,  $x \in \mathcal{X}$ ,  $y \in \mathcal{Y}$ , in residue classes, where  $\mathcal{X}$  and  $\mathcal{Y}$  are sets of the same type as in Theorem 16. Combining this with an elementary sieve, it has been shown in [63] that the set of slightly modified Farey fractions of order  $T$ , that is, the set

$$\mathcal{G}(T) = \{r/s \in \mathbb{Q} : \gcd(r, s) = 1, 1 \leq r, s \leq T\},$$

is uniformly distributed in residue classes modulo a prime  $p$  provided  $T \geq p^{1/2+\varepsilon}$  for any fixed  $\varepsilon > 0$ .

In turn, this result has been used in [63] to improve upper bounds of [62] for the Lang–Trotter conjectures on Frobenius traces and Frobenius fields “on average” over a one-parametric family of elliptic curves

$$\mathbb{E}_{A,B}(t) : \quad U^2 = V^3 + A(t)V + B(t)$$

with some polynomials  $A(t), B(t) \in \mathbb{Z}[t]$  when the variable  $t$  is specialised to the elements of  $\mathcal{G}(T)$ . A similar result can also be obtained for the set  $\mathcal{F}(T)$  of “proper” Farey fractions given by (41).

### 5.11 Torsion of Elliptic Curves

A variant of Theorem 13 has been obtained in [148] and applied to estimating torsion of elliptic curves. More precisely, let  $\mathcal{E}$  be an elliptic curve over an algebraic number field  $\mathbb{K}$  of degree  $d$  over  $\mathbb{Q}$ . It is shown in [148] that if  $\mathcal{E}$  contains a point of prime order  $p$  then

$$p \leq d^{3d^2}.$$

### 5.12 Ranks and Selmer Groups of Elliptic Curves

In [213] the bound (37) is used to show that for any elliptic curve  $\mathcal{E}$  of the form

$$\mathcal{E} : \quad Y^2 = X(X^2 + aX + b)$$

where  $a$  and  $b$  are integers satisfying a certain special relation, the sequence of its *quadratic twists*

$$\mathcal{E}_D : \quad DY^2 = X(X^2 + aX + b)$$

is of rank 0 for a positive proportion of squarefree integers  $D$ . We also note that the bound (37) plays an important role in studying the distribution of Selmer groups of similar families of curves, see [208].

### 5.13 Manin Conjecture for Some del Pezzo Surfaces

Theorem 13 has also been obtained in [129, Lemma 1] where is used a tool to derive an asymptotic formula for rational points of bounded height on some del Pezzo surfaces. A 3-dimensional version of Theorem 13 from [82] has been used in [131] for a similar purpose. These asymptotic formulas correspond to the Manin conjecture for these type of varieties.

## 5.14 Frobenius Numbers

Given a vector  $\mathbf{a} = (a_1, \dots, a_s)$  of  $s$  positive integers with  $\gcd(a_1, \dots, a_s) = 1$  we define its *Frobenius Number*  $F(\mathbf{a})$  as the smallest integer  $f_0$  such that any integer  $f > f_0$  can be represented as

$$f = a_1x_1 + \dots + a_sx_s$$

with nonnegative integers  $x_1, \dots, x_s$ , see [155] for the background.

It has been demonstrated in [163, 185, 195] that for the case  $s = 3$  results of the type of Theorem 13 become important in studying the distribution of the values of  $F(\mathbf{a})$ .

We remark that in the case of  $s = 3$  it has been conjectured in [18] that

$$F((a, b, c)) \leq (abc)^{5/8} \quad (42)$$

for all vectors  $(a, b, c)$  except for some explicitly excluded family of vectors; see also [18, Conjecture 1] for an even stronger conjecture. However the conjectured inequality (42) has been disproved in [163], where it is shown that for any  $a$  there are  $\varphi(a)/2$  pairs  $(b, c)$  with  $a < b < c < 2a$  and  $\gcd(a, b, c) = 1$  for which

$$F((a, b, c)) \geq \frac{a^2}{2}.$$

Since  $abc \leq 4a^3$ , this means that the exponent in  $5/8$  in (42) has to be increased up to at least  $2/3$ . Since these vectors are *admissible* in the terminology of [18] it shows that [18, Conjecture 1] fails too.

However one can do even better by using Theorem 13 and taking any pair  $(b, c)$  with  $bc \equiv 1 \pmod{a}$  and  $b, c = a^{3/4+o(1)}$  in the argument of the proof of [163, Theorem 1], getting

$$F((a, b, c)) \geq a^{7/4+o(1)}$$

for such vectors  $(a, b, c)$ . Thus, since  $abc = a^{5/2+o(1)}$ , we conclude that for any  $a$  there are many pairs  $(b, c)$  for which  $5/8$  in the conjecture (42) has to be increased up to  $7/10$ . Clearly these examples are quite sporadic and certainly do not belong to the family of excluded triples from [18]. We also remark that the family of integral vectors of the form

$$(a, b, c) = (df - 1, d, f), \quad d \leq f \leq d^{1+o(1)},$$

as  $d \rightarrow \infty$ , for which  $abc = a^{2+o(1)}$  leads to the inequality

$$F((a, b, c)) \geq ab^{1+o(1)} = (abc)^{3/4+o(1)}.$$

Furthermore, using lower bounds on  $H(x, y, z; \mathbb{N})$ , see [73, 106] one can see that the sequence of  $a = df - 1$  of the above form is quite dense.

In the opposite direction, it is shown in [199] that for any  $a$  and almost all pairs of positive integers  $(b, c)$  with  $\max\{b, c\} \leq a$  we have

$$F((a, b, c)) \leq (abc)^{1/2}.$$

Several other recent results can be found in [3, 4, 38, 89, 187].

## 5.15 Distribution of Solutions of Linear Equations

The paper [64] has introduced the question on the distribution of ratios  $x/m$  associated with the smallest positive solutions  $(x, y)$  to linear equations  $kx - my = 1$ , on average over the coefficients  $k$  and  $m$  in some intervals. In [64] it has been studied via continued fractions, see also [65]. Then, it has been noticed in [87, 157] that results of the type of Theorem 13 provide a simpler and more direct way to investigate the above ratios. Indeed, it is easy to see that this is equivalent to studying the distribution of modular inverses  $k^{-1} \pmod{m}$  which explains the link with Theorem 13 and of course, with Kloosterman sums (2). However this argument does not take any advantage of averaging over  $m$ . It is very plausible that the results about sums of Kloosterman sums, which date back to [127] can be useful for this kind of problem.

**Question 32.** *Improve the error terms in the asymptotic formulas of [64, 65, 87, 157] by using the results of [127] on cancellations in sums of Kloosterman sums, see also [115, Chapter 16] for the guide to the modern results.*

In [177], using some bounds of certain bilinear exponential sums from [67], these results have been extended to the case when the coefficients  $k$  and  $m$  run through arbitrary but sufficiently dense sets of integers.

## 5.16 Coefficients of Cyclotomic Polynomials

Let

$$A(n) = \max_{k=0, \dots, \varphi(n)} |a_n(k)|$$



be the height of the  $n$ th cyclotomic polynomial:

$$\Phi_n(Z) = \sum_{k=0}^{\varphi(n)} a_n(k) Z^k.$$

In [90], Theorem 13 has been used to show that for any  $\varepsilon > 0$  and any sufficiently large prime  $p$  there exist infinitely many pairs  $(q, r)$  of distinct primes such that

$$A(pqr) \geq \left(\frac{2}{3} - \varepsilon\right) p,$$

which disproves a conjecture from [19].

### 5.17 Approximations by Sums of Several Rationals

Following [46, 47], we consider the problem of obtaining an upper bound on the approximation of a real  $\alpha$  by  $s$  rational fractions with denominators at most  $Q$ , that is for

$$\delta_{\alpha,s}(Q) = \min_{1 \leq q_1, \dots, q_s \leq Q} \left| \alpha - \frac{r_1}{q_1} - \dots - \frac{r_s}{q_s} \right|$$

with positive integers  $q_1, \dots, q_s \leq Q$ . The question is motivated by the Dirichlet theorem on rational approximations which corresponds to the case  $s = 1$ .

It is shown in [46, 47] that the results on the distribution of points on  $\mathcal{H}_{a,m}$  and its multivariate analogues are directly related to this question and imply nontrivial bounds on  $\delta_{\alpha,s}(Q)$ .

In particular, it is remarked in [46] that for  $s = 2$  the question of Section 4.3 on visible points on modular hyperbolas becomes relevant and the result of [168] implies [46, Conjecture 5] with any  $\vartheta > 3/4$ .

Furthermore, it is shown in [173] that in some cases, using Theorem 16, one can improve some of the results of [47].

### 5.18 $\mathrm{SL}_2(\mathbb{F}_p)$ Matrices of Bounded Height

For a finite field  $\mathbb{F}_p$  of  $p$  elements and a positive integer  $T \leq (p-1)/2$ , we use  $N_p(T)$  to denote the number of matrices

$$\begin{pmatrix} u & v \\ x & y \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_p)$$

with  $|u|, |v|, |x|, |y| \leq T$  (we assume that  $\mathbb{F}_p$  is represented by the elements of the set  $\{0, \pm 1, \dots, \pm(p-1)/2\}$ ).

Clearly

$$N_p(T) = \sum_{a \in \mathbb{F}_p} \#\mathcal{H}_{a+1,p}(\mathcal{T}, \mathcal{T}) \#\mathcal{H}_{a,p}(\mathcal{T}, \mathcal{T})$$

where  $\mathcal{T} = \{0, \pm 1, \dots, \pm T\}$  and also  $\#\mathcal{H}_{0,p}(\mathcal{T}, \mathcal{T}) = 4T + 1$ .

It has been shown in [1] that using the identity

$$\sum_{a \in \mathbb{F}_p} \#\mathcal{H}_{a,p}(\mathcal{T}, \mathcal{T}) = (2T + 1)^2$$

and Theorem 16, one can derive that

$$N_p(T) = \frac{(2T + 1)^4}{p} + O(T^2 p^{o(1)}),$$

which is nontrivial if  $T \geq p^{1/2+\varepsilon}$  for any fixed  $\varepsilon > 0$  and sufficiently large  $p$ . More general results on the distribution of determinants of  $n$ -dimensional matrices with entries from an arbitrary (but sufficiently large) set  $\mathcal{A} \subseteq \mathbb{F}_p$  are given in [202], see also [203]. We remark that these are  $\mathbb{F}_p$  analogues of the results of similar spirit for matrices over  $\mathbb{Z}$  and algebraic number fields, see [68, 158] and references therein. Furthermore, if one is only interested in the existence of  $\mathrm{SL}_2(\mathbb{F}_p)$  matrices with bounded entries then one can apply the results from [11] about the existence of solutions to congruences

$$axv + byu \equiv c \pmod{m}$$

in prescribed intervals.

## 5.19 Matrix Products and Continued Fractions

A variant of Theorem 13 plays an important role in obtaining an asymptotic formula for the number of products of the matrices

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$$

which are of trace at most  $N$ , see [20]. In turn, this question is related to studying the number of reduced quadratic irrationalities whose continued fraction expansions are of period length at most  $L$ .

Theorem 13 has also been used in [191] to estimate a certain weighted sum over points of  $\overline{\mathcal{H}}_m$  which appears in studying statistical properties of continued fractions of rational numbers from a certain set such as  $a/b$  with  $a, b \geq 1$  and  $a^2 + b^2 \leq R$ , see also [9, 42, 192, 193, 197, 198] for other versions and applications of Theorem 13.

In [150], one can find several results about rational fractions  $a/m$  with partial quotients bounded by a certain parameter  $k$ . The approach of [150] rests on a series of very interesting results about the distribution of points of  $\mathcal{H}_{a,m}$ .

## 5.20 Computing Discrete Logarithms and Factoring

It has been discovered in [165] that the distribution of points on hyperbolas  $\mathcal{H}_{a,m}$  has direct links with analysis of some discrete logarithm algorithms. Namely, analysis of the algorithm from [165] rests on a weaker version of Theorem 16 obtained in [164].

**Question 33.** *Study whether Theorem 16 can be used to improve some of the results of [165].*

A new deterministic integer factorisation algorithm has recently been suggested in [159]. Its analysis depends on a variant of Theorem 13.

# 6 Concluding Remarks

## 6.1 Multivariate Generalisations

Multidimensional variants of the above problems have also been considered and in principle one can use bounds of multidimensional Kloosterman sums (2) to study the distribution of solutions to the congruence

$$x_1 \dots x_s \equiv a \pmod{m} \tag{43}$$

in the same fashion as in the case of two variables. However, it has been shown in [10] that in many cases bounds of multiplicative character sums lead to much stronger results. For example, in [176], using the bounds of Lemma 2, a previous less general version of Lemma 3 and the bound (6), an improvement is given of some results of [5] on the generalised Lehmer problem, see also [214]. Similar ideas have also led in [169] to some other

results on distribution of solutions to (43). For instance, let  $\Delta_{s,a,m}$  denote the discrepancy of the  $s$ -dimensional points

$$\left(\frac{x_1}{m}, \dots, \frac{x_s}{m}\right) \in [0, 1]^s, \quad x_1 \dots x_s \equiv a \pmod{m}, \quad 1 \leq x_1, \dots, x_s \leq m.$$

It is shown in [169] that

$$\Delta_{s,a,m} \leq \begin{cases} m^{-1/2+o(1)} & \text{if } s = 3, \\ m^{-1+o(1)} & \text{if } s \geq 4. \end{cases}$$

As we have mentioned, a multidimensional analogue of Theorem 28 is given in [183]. Using Lemma 3 in its present form one can easily generalise the above results.

We now show how multiplicative characters can be used on the example of counting the number of solutions to the congruence

$$x_1 \dots x_s \equiv a \pmod{m}, \quad 1 \leq x_i \leq X_i, \quad i = 1, \dots, s,$$

for some integers  $X_1, \dots, X_s \geq 1$ , which we denote as  $N_s(a, m; X_1, \dots, X_s)$ .

Assuming that  $\gcd(a, m) = 1$  and using the identity (5), we write

$$N_s(a, m; X_1, \dots, X_s) = \sum_{x_1=1}^{X_1} \dots \sum_{x_s=1}^{X_s} \frac{1}{\varphi(m)} \sum_{\chi \in \Phi_m} \chi(x_1 \dots x_s a^{-1}).$$

Changing the order of summation and separating the contribution from the principal character  $\chi_0$ , which gives the main term  $X_1 \dots X_s / \varphi(m)$ , we obtain

$$\left| N_s(a, m; X_1, \dots, X_s) - \frac{X_1 \dots X_s}{\varphi(m)} \right| \leq \frac{1}{\varphi(m)} \sum_{\substack{\chi \in \Phi_m \\ \chi \neq \chi_0}} \prod_{i=1}^s \left| \sum_{x_i=1}^{X_i} \chi(x_i) \right|.$$

We now assume that  $s \geq 4$ . Then we apply Lemma 2 to  $s-4$  sums in the above (say, for  $i = 5, \dots, s$ ) and then use the Hölder inequality. This leads to the estimate

$$\begin{aligned} & \left| N_s(a, m; X_1, \dots, X_s) - \frac{X_1 \dots X_s}{\varphi(m)} \right| \\ & \leq \frac{1}{\varphi(m)} m^{(s-4)(\nu+1)/4\nu^2+o(1)} \prod_{i=5}^s X_i^{1-1/\nu} \prod_{i=1}^4 \left( \sum_{\substack{\chi \in \Phi_m \\ \chi \neq \chi_0}} \left| \sum_{x_i=1}^{X_i} \chi(x_i) \right|^4 \right)^{1/4}. \end{aligned}$$

We now apply Lemma 3 to the product of 4th powers. Certainly depending on the relative sizes of  $X_1, \dots, X_s$ , Lemma 2 can give better results if applied to different sums and maybe with different values of  $\nu$  for each sum.

In [93, 95] the above approach based on using multiplicative character sums instead of exponential sums has been complemented with a very interesting new ingredient, which is based on the results and ideas of [83, 113]. In particular, it is shown in [95] that

$$N_3(a, m; X_1, X_2, X_3) > 0$$

and if  $m$  is cubefree then also

$$N_4(a, m; X_1, X_2, X_3, X_4) > 0$$

for all but  $o(m)$  residue classes modulo  $m$ , provided that  $X_1 X_2 X_3 > m^{1+\varepsilon}$  and  $X_1 X_2 X_3 X_4 > m^{1+\varepsilon}$ , respectively, for some fixed  $\varepsilon > 0$ . This line of research is very new and promising.

We, however, note that even in the multidimensional case, multiplicative character sum techniques do not always win over the exponential sum approach. For example, it seems that for the results of [49] the bound on Kloosterman sums (2) gives a more powerful and appropriate tool than bounds of multiplicative character sums.

Upper bounds on the number of solutions of the congruence (43) with variables from short intervals are given in [36, 51]. For example, it is shown in [36] that for a prime  $m = p$  and a positive integer

$$h < p^{1/(s^2-1)}$$

there are at most  $h^{o(1)}$  solutions in interval of length  $h$ , that is with  $x_i \in [k_i + h]$ , for some integers  $k_i$ ,  $i = 1, \dots, s$ , see also [37].

It is worth noticing that one has to be careful with posing multidimensional generalisations, which sometimes lead to rather simple questions for  $s \geq 3$  (despite that for  $s = 2$  they are nontrivial at all). For example, it has been noticed in [169] that often such generalisations do not need any analytic technique used in [217] but follow immediately from a very elementary argument.

## 6.2 Generalisations to Other Congruences and Algebraic Domains

We believe that it is interesting to explore how much of the theory developed for modular hyperbolas can be extended to modular circles

$$\mathcal{C}_{a,m} = \{(x, y) : x^2 + y^2 \equiv a \pmod{m}\}.$$

Well-known parallels between the properties of integer points on hyperbolas and circles on the Euclidean plane, suggest that many of the results obtained for  $\mathcal{H}_{a,m}$  can be extended to  $\mathcal{C}_{a,m}$ . We also recall that [109, Lemma 3] gives a version of Theorem 16 for the number of solutions to the congruence

$$x^2 - y^2 \equiv a \pmod{m}, \quad 1 \leq x, y \leq X,$$

on average over  $a$ .

One can also consider the analogue of the question of Section 5.18 for higher dimensional matrices. For example, for it is shown in [1] that for  $T \geq p^{3/4+\varepsilon}$  the number of matrices

$$(x_{ij})_{i,j=1}^n \in \mathrm{SL}_2(\mathbb{F}_p)$$

with  $|x_{ij}| \leq T$ ,  $i, j = 1, \dots, n$ , is asymptotic to its expected value  $T^{n^2}/p$ . This result is based on different arguments which rely on the results of [77, 78] (and in fact apply to a wide class of polynomial equations).

**Question 34.** *Close the gap between the thresholds  $T \geq p^{1/2+\varepsilon}$  for  $n = 2$  and  $T \geq p^{3/4+\varepsilon}$  for  $n \geq 3$ .*

In [112], using bounds of [72] for exponential sums with matrices, the joint distribution of elements of a matrix  $A \in \mathrm{GL}_n(\mathbb{F}_p)$  and its inverse  $A^{-1}$  has been studied. In particular, in [112] some analogues of the result of [17] have been derived.

One of the interesting and still unexplored lines of research is studying function field generalisations, which conceivably should admit results of the same strength or maybe even stronger as in the case of residue rings. For example, a polynomial analogue of the conjecture of [71] could be more accessible.

**Question 35.** Let  $\mathbb{F}_q$  be a finite field of  $q$  elements. Given an irreducible polynomial  $F(X) \in \mathbb{F}_q[X]$  of sufficiently large degree  $d$ , show that for any polynomial  $A(X) \in \mathbb{F}_q[X]$ , relatively prime to  $F(X)$ , there are two irreducible polynomials  $G(X), H(X) \in \mathbb{F}_q[X]$  of degree at most  $d$  such that

$$G(X)H(X) \equiv A(X) \pmod{F(X)}.$$

It is also natural to ask about possible generalisations of Theorems 13 and 16 to matrix equations.

**Question 36.** Obtain asymptotic formulas, individually for every  $n \times n$  matrix  $A$  over  $\mathbb{Z}/m\mathbb{Z}$  and also on average over all such matrices, for the number of solutions of the congruence

$$XY \equiv A \pmod{m}$$

with matrices  $X = (x_{ij})_{i,j=1}^n$  and  $Y = (y_{ij})_{i,j=1}^n$  where  $x_{ij} \in \mathcal{X}_{ij}$ ,  $y_{ij} \in \mathcal{Y}_{ij}$  for some “interesting” sets  $\mathcal{X}_{ij}, \mathcal{Y}_{ij} \subseteq \mathbb{Z}/m\mathbb{Z}$ ,  $i, j = 1, \dots, n$  (for example, when elements belong to prescribed short intervals).

### 6.3 Ratios Instead of Products

Questions about the distribution of points on modular hyperbolas can be reformulated as questions about the distribution of products  $xy$  in residue classes modulo  $m$ . In turn this naturally leads to similar questions about the distribution of ratios  $x/y$  (with  $\gcd(y, m) = 1$ ) in residue classes. Although typographically similar, many aspects of these new questions are very different.

For example, we have already mentioned in Section 3.1 that for any prime  $p$ , any integer  $a$  can easily be shown to be represented as  $x/y \equiv a \pmod{p}$  for some integers  $x$  and  $y$  with  $|x|, |y| \leq p^{1/2}$ , while for the products this statement is not correct and even obtaining a relaxed statements with  $|x|, |y| \leq p^\gamma$  for some  $\gamma < 3/4$  is still an open problem (and apparently is very hard).

Furthermore, by Theorem 13, every integer  $a$  can be represented in the form  $xy \equiv a \pmod{p}$  for some integers  $x$  and  $y$  with  $1 \leq x, y \leq p^{3/4+\varepsilon}$  for any  $\varepsilon$  and sufficiently large  $p$ , while obviously the congruence  $x/y \equiv -1 \pmod{p}$  has no solution with  $1 \leq x, y \leq p/2$ .

On the other hand, in [171], a full analogue of Theorem 16 is given for the ratios  $x/y$  as well, see also [63, 91, 98, 164] and Section 5.10.

Further investigation of distinctions and similarities between these two groups of questions is a very interesting direction of research.

## 6.4 Further Perspectives

Here we mention some results which have not been used in this area, which we believe can lead to some new directions of research.

We have seen that bounds of Kloosterman sums (2) and several other celebrated number theoretic results and techniques, play a prominent role in this field. Still, it is highly important to further extend the scope of number theoretic tools which can be used for studying the points on modular hyperbolas and their generalisations. In particular, it would be very interesting to find new applications of the bounds of very short incomplete Kloosterman sums from [31, 118, 119, 126, 144, 170, 204].

Furthermore, one may expect that the bounds of bilinear sum

$$\sum_{M \leq m \leq 2M} \sum_{X \leq x \leq 2X} \alpha_m \vartheta_x \mathbf{e}_m(ax^{-1}), \quad a \in \mathbb{Z},$$

from [67] (where  $(\alpha_m)$  and  $(\vartheta_x)$  are arbitrary sequences supported on the intervals  $[M, 2M]$  and  $[X, 2X]$ , respectively) can be useful for studying the points on  $\mathcal{H}_{a,m}$  in very general sets on average over moduli  $m$  taken from another general set. One of such applications has been mentioned in Section 5.15.

In the same spirit, finding applications of the bounds of sums of Kloosterman sums (2) to the study of points on  $\mathcal{H}_{a,m}$  would be of great interest, see [115, Chapter 16] for a background on such results.

## References

- [1] O. Ahmadi and I. E. Shparlinski, ‘Distribution of matrices with restricted entries over finite fields’, *Indag. Math.*, **18** (2007), 327–337.
- [2] W. R. Alford, A. Granville and C. Pomerance, ‘There are infinitely many Carmichael numbers’, *Annals Math.*, **139** (1994), 703–722.
- [3] I. M. Aliev and P. M. Gruber, ‘An optimal lower bound for the Frobenius problem’, *J. Number Theory*, **123** (2007), 71–79.
- [4] I. M. Aliev, M. Henk and A. Hinrichs, ‘Expected Frobenius numbers’, *J. Combin. Theory, Ser. A*, **118** (2011), 525–531.



- [5] E. Alkan, F. Stan and A. Zaharescu, ‘Lehmer  $k$ -tuples’, *Proc. Amer. Math. Soc.*, **134** (2006), 2807–2815.
- [6] E. Alkan, M. Xiong and A. Zaharescu, ‘Quotients of values of the Dedekind eta function’, *Math. Ann.*, **342** (2008), 157–176.
- [7] G. E. Andrews, ‘A lower bound for the volume of strictly convex bodies with many boundary lattice points’, *Trans. Amer. Math. Soc.*, **106** (1963), 270–279.
- [8] V. I. Arnold, ‘Statistics of integral polygons’, *Funct. Anal. Appl.*, **14**(2) (1980), 1–3 (in Russian).
- [9] M. O. Avdeeva, ‘On the statistics of partial quotients of finite continued fractions’, *Funktsional. Anal. i Prilozhen. (Transl. as Funct. Anal. Appl.)*, **38**(2) (2004), 1–11 (in Russian).
- [10] A. Ayyad, ‘The distribution of solutions of the congruence  $x_1x_2x_3 \dots x_n \equiv c \pmod{p}$ ’, *Proc. Amer. Math. Soc.*, **127** (1999), 943–950.
- [11] A. Ayyad and T. Cochrane, ‘Lattices in  $\mathbb{Z}^2$  and the congruence  $xy + uv \equiv c \pmod{m}$ ’, *Acta Arith.*, **132** (2008), 127–133.
- [12] A. Ayyad, T. Cochrane and Z. Zheng, ‘The congruence  $x_1x_2 \equiv x_3x_4 \pmod{p}$ , the equation  $x_1x_2 = x_3x_4$  and the mean value of character sums’, *J. Number Theory*, **59** (1996), 398–413.
- [13] A. Balog and J.-M. Deshouillers, ‘On some convex lattice polygons’, *Number Theory in Progress*, W. de Gruyter, 1999, 591–606.
- [14] R. C. Baker, ‘Kloosterman sums with prime variable’, *Preprint*, 2011.
- [15] W. D. Banks, D. R. Heath-Brown and I. E. Shparlinski, ‘On the average value of divisor sums in arithmetic progressions’, *Intern. Math. Research Notices*, **2005** (2005), 1–25.
- [16] I. Bárány and J. Pach, ‘On the number of convex lattice polygons’, *Combinatorics, Probability, and Computing*, **1** (1992), 295–302.
- [17] J. Beck and M. R. Khan, ‘On the uniform distribution of inverses modulo  $n$ ’, *Period. Math. Hung.*, **44** (2002), 147–155.

- [18] M. Beck, D. Einstein, S. Zacks, ‘Some experimental results on the Frobenius problem’, *Experiment. Math.*, **12** (2003), 263–269.
- [19] M. Beiter, ‘Magnitude of the coefficients of the cyclotomic polynomial  $F_{pqr}$ , II’, *Duke Math. J.*, **38** (1971), 591–594.
- [20] F. P. Boca, ‘Products of matrices  $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$  and  $\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$  and the distribution of reduced quadratic irrationals’, *J. Reine Angew. Math.*, **606** (2007), 149–165.
- [21] F. P. Boca, ‘On the distribution of angles between geodesic rays associated with hyperbolic lattice points’, *Quart. J. Math.*, **58** (2007), 281–295.
- [22] F. P. Boca, C. Cobeli and A. Zaharescu, ‘Distribution of lattice points visible from the origin’, *Commun. Math. Phys.*, **213** (2000), 433–470.
- [23] F. P. Boca, C. Cobeli and A. Zaharescu, ‘A conjecture of R. R. Hall on Farey points’, *J. Reine Angew. Math.*, **535** (2001), 207–236.
- [24] F. P. Boca, R. N. Gologan and A. Zaharescu, ‘The statistics of the trajectory of a certain billiard in a at two-torus’, *Comm. Math. Phys.*, **240** (2003), 53–73.
- [25] F. P. Boca and A. Zaharescu, ‘Farey fractions and two-dimensional tori’, *Noncommutative Geometry and Number Theory*, Aspects of Mathematics E37, Vieweg Verlag, Wiesbaden, 2006, 57–77.
- [26] F. P. Boca and A. Zaharescu, ‘On the correlations of directions in the Euclidean plane’, *Trans. Amer. Math. Soc.*, **358** (2006), 1797–1825.
- [27] F. P. Boca and A. Zaharescu, ‘The distribution of the free path lengths in the periodic two-dimensional Lorentz gas in the small-scatterer limit’, *Comm. Math. Phys.*, **269** (2007), 425–471.
- [28] E. Bombieri, ‘On exponential sums in finite fields’, *Amer. J. Math.*, **88** (1966), 71–105.
- [29] E. Bombieri, J. B. Friedlander and H. Iwaniec, ‘Primes in arithmetic progressions to large moduli, III’, *J. Amer. Math. Soc.*, **2** (1989), 215–224.

- [30] J. Bourgain, ‘Mordell’s exponential sum estimate revisited’, *J. Amer. Math. Soc.*, **18** (2005), 477–499.
- [31] J. Bourgain, ‘More on the sum-product phenomenon in prime fields and its applications’, *Intern. J. Number Theory*, **1** (2005), 1–32.
- [32] J. Bourgain, ‘New encounters in combinatorial number theory: From the Kakeya problem to cryptography’, *Perspectives in Analysis*, Mathematical Physics Studies, Vol. 27, Springer-Verlag, Berlin, 2005, 17–26.
- [33] J. Bourgain, ‘Estimates of polynomial exponential sums’, *Israel J. Math.*, **176** (2010), 221–240.
- [34] J. Bourgain, T. Cochrane, J. Paulhus and C. Pinner, ‘On the parity of  $k$ -th powers modulo  $p$ . A generalization of a problem of Lehmer’, *Acta Arith.*, **147** (2011), 173–203.
- [35] J. Bourgain, T. Cochrane, J. Paulhus and C. Pinner, ‘Decimations of  $l$ -sequences and permutations of even residues mod  $p$ ’, *SIAM J. Discr. Math.*, **23** (2009), 842–857.
- [36] J. Bourgain, M. Z. Garaev, S. V. Konyagin and I. E. Shparlinski, ‘On the hidden shifted power problem’, *Preprint*, 2011 (available from <http://arxiv.org/abs/1110.0812>)
- [37] J. Bourgain, M. Z. Garaev, S. V. Konyagin and I. E. Shparlinski, ‘On congruences with products of variables from short intervals and applications’, *Preprint*, 2012 (available from <http://arxiv.org/abs/1203.0017>).
- [38] J. Bourgain and Y. G. Sinai, ‘Limiting behavior of large Frobenius numbers’, *Uspekhi Matem. Nauk (Transl. as Russian Math. Surveys)*, **62**(4) (2007), 77–90 (in Russian).
- [39] P. Brass, W. Moser and J. Pach, *Research problems in discrete geometry*, Springer, New York, 2005.
- [40] T. Browning and A. Haynes, ‘Incomplete Kloosterman sums and multiplicative inverses in short intervals’, *Preprint*, 2012 (available from <http://arxiv.org/abs/1204.6374>).

- [41] V. A. Bykovskii, ‘Asymptotic properties of lattice points  $(a_1, a_2)$  that satisfy the congruence  $a_1 a_2 \equiv l \pmod{q}$ ’, *Analytic number theory and the theory of functions*, 4, Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov., Vol. 112, 1981, 5–25 (in Russian).
- [42] V. A. Bykovskii, ‘An estimate for the dispersion of lengths of finite continued fractions’, *J. Math. Sci.*, **146** (2007), 5634–5643.
- [43] V. A. Bykovskii and A. V. Ustinov, ‘The statistics of particle trajectories in the homogeneous Sinai problem for a two-dimensional lattice’, *Funktsional. Anal. i Prilozhen. (Transl. as Funct. Anal. Appl.)*, **42**(3) (2008), 10–22 (in Russian).
- [44] V. A. Bykovskii and A. V. Ustinov, ‘The statistics of particle trajectories in the inhomogeneous Sinai problem for a two-dimensional lattice’, *Izv. Ross. Akad. Nauk Ser. Mat. (Transl. as Izvestiya. Mathematics)*, **73** (4) (2009), 17–36 (in Russian).
- [45] T. H. Chan, ‘Distribution of difference between inverses of consecutive integers modulo  $p$ ’, *Integers*, **4** (2004), Paper A03, 1–11.
- [46] T. H. Chan, ‘Approximating reals by sums of two rationals’, *J. Number Theory*, **128** (2008), 1182–1194.
- [47] T. H. Chan, ‘Approximating reals by sums of rationals’, *J. Number Theory*, **129** (2009) 316–324.
- [48] T. H. Chan, ‘A short note about difference between inverses of consecutive integers modulo  $p$ ’, *Integers*, **9** (2009), 699–702.
- [49] T. H. Chan, ‘An almost all result on  $q_1 q_2 \equiv c \pmod{q}$ ’, *Monatsh. Math.*, **162** (2011), 29–39.
- [50] T. H. Chan and I. E. Shparlinski, ‘On the concentration of points on modular hyperbolas and exponential curves’, *Acta Arith.*, **142** (2010), 59–66.
- [51] J. Cilleruelo and M. Z. Garaev, ‘Concentration of points on two and three dimensional modular hyperbolas and applications’, *Geom. and Func. Anal.*, **21** (2011), 892–904.

- [52] J. Cilleruelo, M. Z. Garaev, A. Ostafe and I. E. Shparlinski, ‘On the concentration of points of polynomial maps and applications’, *Math. Zeitschrift*, (to appear).
- [53] C. Cobeli, S. M. Gonek and A. Zaharescu, ‘The distribution of patterns of inverses modulo a prime’, *J. Number Theory*, **101** (2003), 209–222.
- [54] C. Cobeli, M. Văjăitu and A. Zaharescu, ‘Average estimates for the number of tuples of inverses mod  $p$  in short intervals’, *Bull. Math. Soc. Sci. Math. Roumanie.*, **43** (2000), 155–164.
- [55] C. Cobeli, M. Văjăitu and A. Zaharescu, ‘Distribution of gaps between the inverses mod  $q$ ’, *Proc. Edinb. Math. Soc.*, **46** (2003), 185–203.
- [56] C. Cobeli and A. Zaharescu, ‘The order of inverses mod  $q$ ’, *Mathematika*, **47** (2000), 87–108.
- [57] C. Cobeli and A. Zaharescu, ‘Generalization of a problem of Lehmer’, *Manuscr. Math.*, **104** (2001), 301–307.
- [58] C. Cobeli and A. Zaharescu, ‘On the distribution of the  $\mathbb{F}_p$ -points on an affine curve in  $r$  dimensions’, *Acta Arithmetica*, **99** (2001), 321–329.
- [59] T. Cochrane, C. Pinner and J. Rosenhouse, ‘Sparse polynomial exponential sums’, *Acta Arith.*, **108** (2003), 37–52.
- [60] T. Cochrane and S. Sih, ‘The congruence  $x_1x_2 \equiv x_3x_4 \pmod{p}$  and mean values of character sums’, *J. Number Theory*, **130** (2010), 767–785.
- [61] T. Cochrane and Z. Zheng, ‘High order moments of character sums’, *Proc. Amer. Math. Soc.*, **126** (1998), 951–956.
- [62] A. C. Cojocaru and C. Hall, ‘Uniform results for Serre’s theorem for elliptic curves’, *Internat. Math. Res. Notices*, **2005** (2005), 3065–3080.
- [63] A. C. Cojocaru and I. E. Shparlinski, ‘Distribution of Farey fractions in residue classes and Lang–Trotter conjectures on average’, *Proc. Amer. Math. Soc.*, **136** (2008), 1977–1986.

- [64] E. I. Dinaburg and Y. G. Sinai, ‘The statistics of the solutions of the integer equation  $ax - by = \pm 1$ ’, *Funktsional. Anal. i Prilozhen. (Transl. as Funct. Anal. Appl.)*, **24**(3) (1990), 1–8 (in Russian).
- [65] D. Dolgopyat, ‘On the distribution of the minimal solution of a linear Diophantine equation with random coefficients’, *Funktsional. Anal. i Prilozhen. (Transl. as Funct. Anal. Appl.)*, **28**(3) (1994), 22–34 (in Russian).
- [66] M. Drmota and R. Tichy, *Sequences, discrepancies and applications*, Springer-Verlag, Berlin, 1997.
- [67] W. Duke, J. B. Friedlander and H. Iwaniec, ‘Bilinear forms with Kloosterman fractions’, *Invent. Math.*, **128** (1997), 23–43.
- [68] W. Duke, Z. Rudnick and P. Sarnak, ‘Density of integer points on affine homogeneous varieties’, *Duke Math. J.*, **71** (1993), 143–179.
- [69] Z. Dvir, ‘On the size of Kakeya sets in finite fields’, *J. Amer. Math. Soc.*, **22** (2009), 1093–1097.
- [70] D. Eichhorn, M. R. Khan, A. H. Stein and C. L. Yankov, ‘Sum and differences of coordinates of points on modular hyperbolas’, *Combinatorial Number Theory, Proc. Integers Confer. 2007*, W. de Gruyter, 2009, 17–39.
- [71] P. Erdős, A. M. Odlyzko and A. Sárközy, ‘On the residues of products of prime numbers’, *Period. Math. Hung.*, **18** (1987), 229–239.
- [72] R. Ferguson, C. Hoffman, F. Luca, A. Ostafe and I. E. Shparlinski, ‘Some additive combinatorics problems in matrix rings’, *Revista Matem. Complutense*, **23** (2010), 501–513.
- [73] K. Ford, ‘The distribution of integers with a divisor in a given interval’, *Annals Math.*, **168** (2008), 367–433.
- [74] K. Ford, M. R. Khan and I. E. Shparlinski, ‘Geometric properties of points on modular hyperbolas’, *Proc. Amer. Math. Soc.*, **138** (2010), 4177–4185.

- [75] K. Ford, M. R. Khan, I. E. Shparlinski and C. L. Yankov, ‘On the maximal difference between an element and its inverse in residue rings’, *Proc. Amer. Math. Soc.*, **133** (2005), 3463–3468.
- [76] É. Fouvry, ‘Sur le problème des diviseurs de Titchmarsh’, *J. Reine Angew. Math.*, **357** (1985), 51–76.
- [77] É. Fouvry, ‘Consequences of a result of N. Katz and G. Laumon concerning trigonometric sums’, *Israel J. Math.*, **120** (2000), 81–96.
- [78] É. Fouvry and N. M. Katz, ‘A general stratification theorem for exponential sums, and applications’, *J. Reine Angew. Math.*, **540** (2001), 115–166.
- [79] É. Fouvry and P. Michel, ‘Sur certaines sommes d’exponentielles sur les nombres premiers’, *Ann. Sci. École Norm. Sup.*, **31** (1998), 93–130.
- [80] É. Fouvry and I. Shparlinski, ‘On a ternary quadratic form over primes’, *Acta Arith.*, **150** (2011), 285–314.
- [81] É. Fouvry and I. Shparlinski, ‘Smooth shifted monomial products’, *Publ. Math. Debrecen*, **79** (2011), 423–432.
- [82] J. B. Friedlander and H. Iwaniec, ‘Incomplete Kloosterman sums and a divisor problem’, *Ann. Math.*, **121** (1985), 319–350.
- [83] J. B. Friedlander and H. Iwaniec, ‘The divisor problem for arithmetic progressions’, *Acta Arith.*, **45** (1985), 273–277.
- [84] J. B. Friedlander, P. Kurlberg and I. E. Shparlinski, ‘Products in residue classes’, *Math. Res. Letters*, **15** (2008), 1133–1147.
- [85] J. B. Friedlander and F. Luca, ‘Residue classes having tardy totients’, *Bull. Lond. Math. Soc.*, **40** (2008), 1007–1016.
- [86] J. B. Friedlander and I. E. Shparlinski, ‘Least totient in a residue class’, *Bull. Lond. Math. Soc.*, **39** (2007), 425–432.
- [87] A. Fujii, ‘On a problem of Dinaburg and Sinai’, *Proc. Japan Acad. Sci., Ser. A*, **68** (1992), 198–203.

- [88] A. Fujii and Y. Kitaoka, ‘On plain lattice points whose coordinates are reciprocals modulo a prime’, *Nagoya Math. J.*, **147** (1997), 137–146.
- [89] L. Fukshansky and S. Robins, ‘Frobenius problem and the covering radius of a lattice’, *Discrete Comput. Geom.*, **37** (2007), 471–483.
- [90] Y. Gallot and P. Moree, ‘Ternary cyclotomic polynomials having a large coefficient’, *J. Reine Angew. Math.*, **632** (2009), 105–125.
- [91] M. Z. Garaev, ‘Character sums in short intervals and the multiplication table modulo a large prime’, *Monatsh. Math.*, **148** (2006), 127–138.
- [92] M. Z. Garaev, ‘On the logarithmic factor in error term estimates in certain additive congruence problems’, *Acta Arith.*, **124** (2006), 27–39.
- [93] M. Z. Garaev, ‘A note on the least totient of a residue class’, *Quart. J. Math.*, **60** (2009), 53–56.
- [94] M. Z. Garaev, ‘Estimation of Kloosterman sums with prime numbers and an application’, *Matem. Zametki*, **88** (2010), 365–373, (in Russian).
- [95] M. Z. Garaev, ‘On multiplicative congruences’, *Math. Zeitschrift*, (to appear).
- [96] M. Z. Garaev and V. C. Garcia, ‘The equation  $x_1x_2 = x_3x_4 + \lambda$  in fields of prime order and applications’, *J. Number Theory*, **128** (2008), 2520–2537.
- [97] M. Z. Garaev and A. A. Karatsuba, ‘On character sums and the exceptional set of a congruence problem’, *J. Number Theory*, **114** (2005), 182–192.
- [98] M. Z. Garaev and A. A. Karatsuba, ‘The representation of residue classes by products of small integers’, *Proc. Edinburgh Math. Soc.*, **50** (2007), 363–375.
- [99] M. Z. Garaev and K.-L. Kueh, ‘Distribution of special sequences modulo a large prime’, *Int. J. Math. Math. Sci.*, **50** (2003), 3189–3194.



- [100] S. M. Gonek, G. S. Krishnaswami and V. L. Sondhi, ‘The distribution of inverses modulo a prime in short intervals’, *Acta Arith.*, **102** (2002), 315–322.
- [101] M. Goresky and A. Klapper, ‘Arithmetic cross-correlations of FCSR sequences’, *IEEE Trans. Inform. Theory*, **43** (1997), 1342–1346.
- [102] M. Goresky, A. Klapper, R. Murty and I. E. Shparlinski, ‘On decimations of  $\ell$ -sequences’, *SIAM J. Discrete Math.*, **18** (2004), 130–140.
- [103] A. Granville, I. E. Shparlinski and A. Zaharescu, ‘On the distribution of rational functions along a curve over  $\mathbb{F}_p$  and residue races’, *J. Number Theory*, **112** (2005), 216–237.
- [104] R. K. Guy, *Unsolved problems in number theory*, Springer-Verlag, Berlin, 1994.
- [105] L. Guth and N. H. Katz, ‘On the Erdos distinct distance problem in the plane’, *Preprint*, 2011 (available from <http://arxiv.org/abs/1011.4105>).
- [106] R. R. Hall and G. Tenenbaum, *Divisors*, Cambridge Tracts in Math., Vol. 90, Cambridge Univ. Press, 1988.
- [107] S. Hanrahan and M. R. Khan, ‘The cardinality of the value sets modulo  $n$  of  $x^2 + x^{-2}$  and  $x^2 + y^2$ ’, *Involve*, **3** (2010), 171–182.
- [108] D. R. Heath-Brown, ‘The divisor function  $d_3(n)$  in arithmetic progressions’, *Acta Arith.*, **47** (1986), 29–56.
- [109] D. R. Heath-Brown, ‘Pair correlation for fractional parts of  $\alpha n^2$ ’, *Math. Proc. Camb. Phil. Soc.*, **148** (2010), 385–407.
- [110] C. Hooley, ‘An asymptotic formula in the theory of numbers’, *Proc. London Math. Soc.*, **7** (1957), 396–413.
- [111] C. Hooley, ‘On the greatest prime factor of a cubic polynomial’, *J. Reine Angew. Math.*, **303/304** (1978) 21–50.
- [112] S. Hu and Y. Li, ‘On a uniformly distributed phenomena in matrix groups’, *Preprint*, 2011 (available from <http://arxiv.org/abs/1103.3928>).

- [113] M. N. Huxley, ‘Large values of Dirichlet polynomials, III’, *Acta Arith.*, **26** (1974), 435–444.
- [114] M. Huxley and M. Jutila, ‘Large values of Dirichlet polynomials, IV’, *Acta Arith.*, **32** (1977), 297–312.
- [115] H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer. Math. Soc., Providence, RI, 2004.
- [116] M. Jutila, ‘Zero-density estimates for L-functions’, *Acta Arith.*, **32** (1977), 55–62.
- [117] A. A. Karatsuba, ‘Sums of characters with prime numbers’, *Izv. Akad. Nauk Ser. Mat.*, **34** (1970) 299–321.
- [118] A. A. Karatsuba, ‘Fractional parts of functions of a special form’, *Izv. Ross. Akad. Nauk Ser. Mat. (Transl. as Russian Acad. Sci. Izv. Math.)*, **59**(4) (1995), 61–80 (in Russian).
- [119] A. A. Karatsuba, ‘Analogues of Kloosterman sums’, *Izv. Ross. Akad. Nauk Ser. Mat. (Transl. as Russian Acad. Sci. Izv. Math.)*, **59**(5) (1995), 93–102 (in Russian).
- [120] N. Katz and T. Tao, ‘Recent progress on the Keakeya conjecture’, *Proceedings of the 6th International Conference on Harmonic Analysis and Partial Differential Equations* Publ Matem., U. Barcelona, 2002, 161–180.
- [121] M. R. Khan, ‘Problem 10736: An optimization with a modular constraint’, *Amer. Math. Monthly*, **108** (2001), 374–375.
- [122] M. R. Khan, ‘Modular hyperbolas and the coefficients of  $(x^{-1}+6+x)^k$ ’, *Integers*, **11** (2011), 469–476.
- [123] M. R. Khan and I. E. Shparlinski, ‘On the maximal difference between an element and its inverse modulo  $n$ ’, *Period. Math. Hung.*, **47** (2003), 111–117.
- [124] M. R. Khan, I. E. Shparlinski and C. L. Yankov, ‘On the convex closure of the graph of modular inversions’, *Experimental Math.*, **17** (2008), 91–104.

- [125] S. V. Konyagin and I. E. Shparlinski, ‘On convex hull of points on modular hyperbolas’, *Moscow J. Comb. and Number Theory*, **1** (2011), 43–51.
- [126] M. A. Korolev, ‘Incomplete Kloosterman sums and their applications’, *Izv. Ross. Akad. Nauk Ser. Mat. (Transl. as Izvestiya. Mathematics)*, **64**(6) (2000), 41–64 (in Russian).
- [127] N. V. Kuznetsov, ‘The Peterson conjecture for cusp forms of weight zero and the Linnik conjecture. Sums of Kloosterman sums’, *Matem. Sbornik (Transl. as Sbornik: Mathematics)*, **111** (1980), 334–383 (in Russian).
- [128] M. Laczkovich, ‘Discrepancy estimates for sets with small boundary’, *Studia Sci. Math. Hungar.*, **30** (1995), 105–109.
- [129] P. Le Boudec, ‘Manin’s conjecture for two quartic del Pezzo surfaces with  $3A_1$  and  $A_1 + A_2$  singularity types’, *Acta Arith.*, **151** (2012), 109–163.
- [130] P. Le Boudec, ‘Power-free values of the polynomial  $t_1 \dots t_r - 1$ ’, *Bull. Aust. Math. Soc.*, **85** (2012), 154–163.
- [131] P. Le Boudec, ‘Manin’s conjecture for a cubic surface with  $2A_2 + A_1$  singularity type’, *Proc. Cambridge Philos. Soc.*, (to appear).
- [132] H. N. Liu, ‘A note on Lehmer  $k$ -tuples’, *Intern. J. Number Theory*, **5** (2009), 1169–1178.
- [133] H. N. Liu and W. Zhang, ‘On a problem of D. H. Lehmer’, *Acta Math. Sinica*, **22** (2006), 61–68.
- [134] H. N. Liu and W. Zhang, ‘Hybrid mean value on the difference between a quadratic residue and its inverse modulo  $p$ ’, *Publ. Math. Debrecen*, **69** (2006), 227–243.
- [135] H. N. Liu and W. Zhang, ‘General Kloosterman sums and the difference between an integer and its inverse modulo  $q$ ’, *Acta Math. Sinica*, **23** (2007), 77–82.

- [136] H. N. Liu and W. Zhang, ‘Mean value on the difference between a quadratic residue and its inverse modulo  $p$ ’, *Acta Math. Sinica*, **23** (2007), 915–924.
- [137] H. N. Liu and W. Zhang, ‘Hybrid mean value results for a generalization on a problem of D. H. Lehmer and hyper-Kloosterman sums’, *Osaka J. Math.*, **44** (2007), 615–637.
- [138] H. N. Liu and W. Zhang, ‘Hybrid mean value on the difference between an integer and its inverse modulo  $q$ ’, *Archiv Math.*, **46** (2008), 337–347.
- [139] S. R. Louboutin, J. Rivat and A. Sárközy, ‘On a problem of D. H. Lehmer’, *Proc. Amer. Math. Soc.*, **135** (2007), 969–975.
- [140] Y. Lu and Y. Yi, ‘On the generalization of the D. H. Lehmer problem’, *Acta Math. Sinica*, **25** (2009), 1269–1274.
- [141] Y. Lu and Y. Yi, ‘On the generalization of the D. H. Lehmer problem, II’, *Acta Arith.*, **142** (2010), 179–186.
- [142] Y. Lu and Y. Yi, ‘Partitions involving D. H. Lehmer numbers’, *Monatsh. Math.*, **159** (2010), 45–58.
- [143] Y. Lu and Y. Yi, ‘A note on the D. H. Lehmer problem over short intervals’, *Acta Math. Sinica*, **27** (2011), 1115–1120.
- [144] W. Luo, ‘Bounds for incomplete hyper-Kloosterman sums’, *J. Number Theory*, **75** (1999), 41–46.
- [145] K.-H. Mak and A. Zaharescu, ‘Lehmer points and visible points on affine varieties over finite fields’, *Preprint*, 2011 (available from <http://arxiv.org/abs/1110.4691>).
- [146] J. Marklof and A. Strömbergsson, ‘Equidistribution of Kronecker sequences along closed horocycles’, *Geom. Funct. Analysis*, **13** (2003), 1239–1280.
- [147] K. Matomäki, ‘On the greatest prime factor of  $ab + 1$ ’, *Acta Math. Hung.*, **124** (2009), 115–123.

- [148] L. Merel, ‘Bornes pour la torsion des courbes elliptiques sur les corps de nombres’, *Invent. Math.*, **124** (1996), 437–449.
- [149] N. G. Moshchevitin, ‘On numbers with missing digits: Solvability of the congruences  $x_1x_2 \equiv \lambda \pmod{p}$ ’, *Doklady Akad. Nauk (Transl. as Doklady Mathematics)*, **410** (2006), 730–733 (in Russian).
- [150] N. G. Moshchevitin, ‘Sets of the form  $\mathcal{A} + \mathcal{B}$  and finite continued fractions’, *Matem. Sbornik (Transl. as Sbornik: Mathematics)*, **198**(4) (2007), 95–116 (in Russian).
- [151] N. G. Moshchevitin and I. D. Shkredov, ‘On the multiplicative properties modulo  $m$  of numbers with missing digits’, *Mathem. Zametki (Transl. as Math. Notes)*, **81** (2007), 385–404 (in Russian).
- [152] H. Niederreiter and J. M. Wills, ‘Diskrepanz und Distanz von Massen bezüglich konvexer und Jordanscher Mengen’, *Math. Z.*, **144** (1975), 125–134.
- [153] F. V. Petrov, ‘Estimates for the number of rational points on convex curves and surfaces’, *Zapiski Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI)*, **344** (2007), 174–189 (in Russian).
- [154] Z. Kh. Rakhmonov, ‘On the distribution of values of Dirichlet characters and their applications’, *Proc. Steklov Inst. Math.*, **207** (1995) 263–272.
- [155] J. L. Ramírez Alfonsín, *The Diophantine Frobenius problem*, Oxford Lecture Series in Math. and its Appl., Vol. 30, Oxford Univ. Press, Oxford, 2005.
- [156] A. Rényi and R. Sulanke, ‘Über die Konvexe Hülle von  $n$  Zufällig Gewählten Punkten’, *Z. Wahrscheinlichkeitstheorie*, **2** (1963), 75–84.
- [157] G. J. Rieger, ‘Über die Gleichung  $ad - bc = 1$  und Gleichverteilung’, *Math. Nachr.*, **162** (1993), 139–143.
- [158] C. Roettger, ‘Counting invertible matrices and uniform distribution’, *J. Théorie Nombres Bordeaux*, **17** (2005), 301–322.

- [159] M. Rubinstein, ‘Hide and seek – A naive factoring algorithm’, *Preprint*, 2006 (available from <http://arxiv.org/abs/math/0610612>).
- [160] Z. Rudnick and P. Sarnak, ‘The distribution of spacings between the fractional parts of  $n^2\alpha$ ’, *Invent. Math.*, **145** (2001), 37–57.
- [161] I. Z. Ruzsa and A. Schinzel, ‘An application of Kloosterman sums’, *Compos. Math.*, **96** (1995), 323–330.
- [162] É. Saias, ‘Entiers á diviseurs denses 1’, *J. Number Theory*, **62** (1997), 163–191.
- [163] J.-C. Schlage-Puchta, ‘An estimate for Frobenius’ Diophantine problem in three dimensions’, *J. Integer Sequences*, **8** (2005), Article 05.1.7, 1–4 (available from <http://www.cs.uwaterloo.ca/journals/JIS/vol8.html>).
- [164] I. A. Semaev, ‘On the number of small solutions of a linear homogeneous congruence’, *Mat. Zametki (Transl. as Math. Notes)*, **50**(4) (1991), 102–107, (in Russian).
- [165] I. A. Semaev, ‘An algorithm for evaluation of discrete logarithms in some nonprime finite fields’, *Math. Comp.*, **67** (1998), 1679–1689.
- [166] V. Shelestunova, ‘Upper bounds for the number of integral points on quadratic curves and surfaces’, *PhD Thesis*, University of Waterloo, Ontario, Canada, 2010.
- [167] I. E. Shparlinski, ‘On exponential sums with sparse polynomials and rational functions’, *J. Number Theory*, **60** (1996), 233–244.
- [168] I. E. Shparlinski, ‘Primitive points on a modular hyperbola’, *Bull. Polish Acad. Sci. Math.*, **54** (2006), 193–200.
- [169] I. E. Shparlinski, ‘On the distribution of points on multidimensional modular hyperbolas’, *Proc. Japan Acad. Sci., Ser.A*, **83** (2007), 5–9.
- [170] I. E. Shparlinski, ‘Bounds of incomplete multiple Kloosterman sums’, *J. Number Theory*, **126** (2007), 68–73.

- [171] I. E. Shparlinski, ‘Distribution of inverses and multiples of small integers and the Sato–Tate conjecture on average’, *Michigan Math. J.*, **56** (2008), 99–111.
- [172] I. E. Shparlinski, ‘On the Euler function on differences between the coordinates of points on modular hyperbolas’, *Bull. Polish Acad. Sci. Math.*, **56** (2008), 1–7.
- [173] I. E. Shparlinski, ‘Approximation by several rationals’, *Bull. Aust. Math. Soc.*, **77** (2008), 325–329.
- [174] I. E. Shparlinski, ‘On a generalised Lehmer problem for arbitrary powers’, *Contributions in General Algebra II*, Bangkok, 2008, 197–216.
- [175] I. E. Shparlinski, ‘On some weighted average values of  $L$ -functions’, *Bull. Aust. Math. Soc.*, **79** (2009), 183–186.
- [176] I. E. Shparlinski, ‘On a generalisation of a Lehmer problem’, *Math. Zeitschrift*, **263** (2009), 619–631.
- [177] I. E. Shparlinski, ‘On the distribution of solutions to linear equations’, *Glasnik Math.*, **44** (2009), 7–10.
- [178] I. E. Shparlinski, ‘On the restricted divisor function in arithmetic progressions’, *Revista Matemática Iberoamer.*, **28** (2012), 231–238.
- [179] I. E. Shparlinski, ‘On small solutions to quadratic congruences’, *J. Number Theory*, **131** (2011), 1105–1111.
- [180] I. E. Shparlinski, ‘On products of primes and almost primes in arithmetic progressions’, *Period. Math. Hungarica*, (to appear).
- [181] I. E. Shparlinski and J. F. Voloch, ‘Visible points on curves over finite fields’, *Bull. Polish Acad. Sci. Math.*, **55** (2007), 193–199.
- [182] I. E. Shparlinski and A. Winterhof, ‘On the number of distances between the coordinates of points on modular hyperbolas’, *J. Number Theory*, **128** (2008), 1224–1230.

- [183] I. E. Shparlinski and A. Winterhof, ‘Visible points on multidimensional modular hyperbolas’, *J. Number Theory*, **128** (2008), 2695–2703.
- [184] I. E. Shparlinski and A. Winterhof, ‘Partitions into two Lehmer numbers’, *Monat. Math.*, **160** (2010), 429–441.
- [185] V. Shchur, Y. G. Sinai and A. V. Ustinov, ‘Limiting distribution of Frobenius numbers for  $n = 3$ ’, *J. Number Theory*, **129** (2009), 2778–2789.
- [186] C. L. Stewart, ‘On the greatest prime factor of integers of the form  $ab + 1$ ’, *Period. Math. Hung.*, **43** (2001), 81–91.
- [187] Z. Šunić, ‘Frobenius problem and dead ends in integers’, *J. Number Theory*, **128** (2008), 1211–1223.
- [188] R. Taylor, ‘Automorphy for some  $l$ -adic lifts of automorphic mod  $l$  Galois representations, II’, *Pub. Math. IHES*, **108** (2008), 183–239.
- [189] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge Univ. Press, 1995.
- [190] J. L. Truelsen, ‘Divisor problems and the pair correlation for the fractional parts of  $n^2\alpha$ ’, *Intern. Math. Research Notices*, **2010** (2010), 3144–3183.
- [191] A. V. Ustinov, ‘On statistical properties of finite continued fractions’, *J. Math. Sci.*, **137** (2006), 4722–4738.
- [192] A. V. Ustinov, ‘Calculation of the variance in a problem in the theory of continued fractions’, *Matem. Sb. (Transl. as Sbornik: Mathematics)*, **198**(6) (2007), 139–158 (in Russian).
- [193] A. V. Ustinov, ‘Asymptotic behaviour of the first and second moments of the number of steps in the Euclid algorithm’, *Izv. Ross. Akad. Nauk Ser. Mat. (Transl. as Izvestiya. Mathematics)*, **72**(5) (2008), 189–224 (in Russian).
- [194] A. V. Ustinov, ‘On the number of solutions of the congruence  $a_1a_2 \equiv l \pmod{q}$  under the graph of a twice differentiable function’, *Algebra and Analysis*, **20**(5) (2008), 186–216 (in Russian).



- [195] A. V. Ustinov, ‘The solution of Arnolds problem on the weak asymptotics of Frobenius numbers with three arguments’, *Matem. Sb. (Transl. as Sbornik: Mathematics)*, **200**(4) (2009), 131–160 (in Russian).
- [196] A. V. Ustinov, ‘On the distribution of integer points’, *Dalnevostochnyi Matem. J. (Far Eastern Math. J.)*, **9**(1-2) (2009), 176–181 (in Russian).
- [197] A. V. Ustinov, ‘The mean number of steps in the Euclidean algorithm with least absolute-value remainders’, *Mathem. Zametki (Transl. as Math. Notes)*, **85** (2009), 153–156 (in Russian).
- [198] A. V. Ustinov, ‘On the statistical properties of elements of continued fractions’, *Doklady Akad. Nauk (Transl. as Doklady Mathematics)*, **424** (2009), 459–461 (in Russian).
- [199] A. V. Ustinov, ‘On the distribution of Frobenius numbers with three arguments’, *Izv. Ross. Akad. Nauk Ser. Mat. (Transl. as Izvestiya. Mathematics)*, **74**(5) (2010) 145–170 (in Russian).
- [200] M. Văjăitu and A. Zaharescu, ‘Distribution of values of rational maps on the  $\mathbb{F}_p$ -points on an affine curve’, *Monatsh. Math.*, **136** (2002), 81–86.
- [201] R. C. Vaughan and T. D. Wooley, ‘Further improvements in Waring’s problem’, *Acta Math.*, **174** (1995), 147–240.
- [202] L. A. Vinh, ‘On the distribution of determinant of matrices with restricted entries over finite fields’, *J. Combin. and Number Theory*, **1** (2010), 203–212.
- [203] L. A. Vinh, ‘On the distribution of permanents of matrices over finite fields’, *Electronic Notes in Discr. Math* **34** (2009), 519–523.
- [204] Y. Wang and H. Li, ‘On  $s$ -dimensional incomplete Kloosterman sums’, *J. Number Theory*, **130** (2010), 1602–1608.
- [205] Y. Weili, ‘On the generalization of the D. H. Lehmer problem and its mean value’, *J. Algebra, Number Theory and Appl.*, **6** (2006), 479–491.

- [206] H. Weyl, ‘On the volume of tubes’, *Amer. J. Math.*, **61** (1939), 461–472.
- [207] P. Xi and Y. Yi, ‘Generalized D. H. Lehmer problem over short intervals’, *Glasgow Math. J.*, **53** (2011), 293–299.
- [208] M. Xiong and A. Zaharescu, ‘Distribution of Selmer groups of quadratic twists of a family of elliptic curves’, *Advances Math.*, **219** (2008), 523–553.
- [209] Z. Xu, ‘D. H. Lehmer problem over half intervals’, *J. Korean Math. Soc.*, **46** (2009), 493–511.
- [210] Z. Xu and W. Zhang, ‘On a problem of D. H. Lehmer over short intervals’, *J. Math. Anal. Appl.*, **320** (2006), 756–770.
- [211] Z. Xu and W. Zhang, ‘A problem of D. H. Lehmer and its mean value’, *Math. Nachr.*, **281** (2008), 596–606.
- [212] Y. Yi and W. Zhang, ‘On the generalization of a problem of D. H. Lehmer’, *Kyushu J. Math.*, **56** (2002), 235–241.
- [213] G. Yu, ‘Rank 0 quadratic twists of a family of elliptic curves’, *Compos. Math.*, **135** (2003), 331–356.
- [214] Y. Yuan and H. Yiwei, ‘On a generalisation of D. H. Lehmer problem’, *J. of Algebra, Number Theory and Appl.*, **14** (2009), 37–50.
- [215] A. Zaharescu, ‘The distribution of the values of a rational function modulo a big prime’, *J. Theor. Nombres Bordeaux*, **15** (2003), 863–872.
- [216] T. Zhang and X. Xue, ‘On the  $r$ -th hyper-Kloosterman sums and a problem of D. H. Lehmer’, *J. Korean Math. Soc.*, **46** (2009), 733–746.
- [217] T. Zhang and W. Zhang, ‘A generalization on the difference between an integer and its inverse modulo  $q$ , II’, *Proc. Japan Acad. Sci., Ser. A*, **81** (2005), 7–11.
- [218] W. Zhang, ‘On a problem of D. H. Lehmer and its generalization’, *Compos. Math.*, **86** (1993), 307–316.

- [219] W. Zhang, ‘On a problem of D. H. Lehmer and its generalization, II’, *Compos. Math.*, **91** (1994), 47–56.
- [220] W. Zhang, ‘On the difference between a D. H. Lehmer number and its inverse modulo  $q$ ’, *Acta Arith.*, **68** (1994), 255–263.
- [221] W. Zhang, ‘On the difference between an integer and its inverse modulo  $n$ ’, *J. Number Theory*, **52** (1995), 1–6.
- [222] W. Zhang, ‘On the distribution of inverses modulo  $n$ ’, *J. Number Theory*, **61** (1996), 301–310.
- [223] W. Zhang, ‘On a problem of P. Gallagher’, *Acta Math. Hung.*, **78** (1998), 345–357.
- [224] W. Zhang, ‘On the distribution of inverses modulo  $p$ , II’, *Acta Arith.*, **100** (2001), 189–194.
- [225] W. Zhang, ‘On a problem of D. H. Lehmer and Kloosterman sums’, *Monatsh. Math.*, **139** (2003), 247–257.
- [226] W. Zhang, ‘On the mean value of  $L$ -functions with the weight of character sums’, *J. Number Theory*, **128** (2008), 2459–2466.
- [227] W. Zhang, Z. Xu and Y. Yi, ‘A problem of D. H. Lehmer and its mean square value formula’, *J. Number Theory*, **103** (2003), 197–213.
- [228] W. Zhang and Y. Yi, ‘Some applications of Bombieri’s estimate for exponential sums’, *Acta Arith.*, **107** (2003), 245–250.
- [229] Z. Zheng, ‘The distribution of zeros of an irreducible curve over a finite field’, *J. Number Theory*, **59** (1996), 106–118.
- [230] Z. Zheng and T. Cochrane, ‘Distribution of primitive  $\lambda$ -roots of composite moduli II’, *Chinese Annals of Math., Ser. B*, **27** (2006), 549–552.